

Model 1200 series SecureSync/9400 series

Note: This document contains both “Public Information” and “Internal Use Only Information” (do not release this document in its entirety to anyone outside of Orolia)

Table of Contents

MODEL 1200 SERIES SECURESYNC/9400 SERIES	1
GENERAL SAFETY	13
SAFETY: REGULATORY COMPLIANCE: UL / FCC/ EMC-ESD / EMI / CB TESTING / ROHS-CE / COMPLIANCE / DECLARATION OF CONFORMITY (DoC)/IEC-60950-1/IEC-62368/EN 55032	15
CE DECLARATION OF CONFIRMITY (DoC) FOR SECURESYNC/9400s	15
LEAKAGE CURRENT (CURRENT LEAKAGE)	15
FLAMMABILITY TESTING/CERTIFICATION	15
EMI-EMISSIONS/EMC/ESD TESTING	16
UL TESTING/ UL CERTIFICATES	16
***TOUCH CURRENT	16
ROHS COMPLIANCY STATEMENT FOR SECURESYNCS AND 9400s	17
MIL-STD-461 (ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS)	19
ARTICLE 3.2 OF THE EU RADIO EQUIPMENT DIRECTIVE (RED) / ETSI EN 303 417: WIRELESS POWER TRANSMISSION SYSTEMS (WPT)	20
DISA/STIGS (SECURITY TECHNICAL IMPLEMENTATION GUIDES)/SRGs (SECURITY REQUIREMENTS GUIDES) FOR ALL PRODUCTS	23
INFORMATION ASSURANCE (IA) / COMMON CRITERIA (CC) / EAL LEVELS	28
FIPS COMPLIANCY (FIPS 140-2) /CIP/NERC/CYBER SECURITY/POTENTIAL VULNERABILITIES/ANTI-VIRUS SOFTWARE/ CSG SECURITY ACCREDITATION	29
**GENERAL RECOMMENDATIONS FOR VULNERABILITY TESTING	35
SECURITY HARDENING: PCI-DSS / PCI COMPLIANCE/PCI AUDITS (PAYMENT CARD INDUSTRY) SECURITY ASSESSMENTS/PCI DSS AUDITS/ NERC CIP-007 AND CIP-010	37
ISO 8601 (ISO-8601) COMPLIANCY (INTERNATIONALLY ACCEPTED WAY TO REPRESENT DATES AND TIMES)	40
IEC 60945 (MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS)	40
IEC 61850 (ELECTRICAL SUBSTATION AUTOMATION SPECIFICATIONS)	41
VOLUNTARY PRODUCT ACCESSIBILITY TEMPLATE (VPAT)”.SECTION 508 FORM / FORM 508 OF THE REHABILITATION ACT (FOR PEOPLE WITH DISABILITIES: BLIND, HEARING IMPAIRED. ETC)	42
JAPANESE SAFETY COMPLIANCE (ROHS/UL94HB/ INORGANIC PHOSPHORUS/ESD TOLERANCE DATA OR ESD LEVEL)	42
"INDIAN TRUSTED TELECOM PORTAL"	42
SCADA SYSTEMS	43
Y2K38 (YEAR 2038 ROLLOVER) (“UNIX MILLENNIUM BUG”)	43
FAA/BOEING/USAF FLIGHT QUALIFICATION CERTIFICATON TESTING	44
LAFAYETTE (MODEL 1200 SERIES SECURESYNC)	45
LINKS/SHORTCUTS:	45
LAST TIME BUY (LTB) / END OF LIFE (EOL) / DISCONTINUANCE OF 1200 SECURESYNCS	46
SECURESYNC TECH BRIEF: 1200 SECURESYNC TO 2400 SECURESYNC MIGRATION GUIDE	48
SPECTRACOM PRODUCT ROADMAPS	48
INTERNATIONAL SHIPPING/EXPORT CONTROL (ECCN, CCATS AND HTS CODES) FOR SECURESYNCS AND NETCLOCK 9400s	48
REPAIRS/SAASM RMAs	50
OGSI SUPPORTED PRODUCTS	50
MTBF/MTTR	50
REAR PANEL/SLOTS-SLOT NUMBERING	51
IN-HOUSE SECURESYNC REFERENCES FOR ENGINEERING	52
SECURESYNCS/MODEL 9483s ON THE INTERNET (OUTSIDE OF FIREWALL)	53
VISIO STENCILS/SHAPES	54
DATA SHEET /SPECS	55
LAFAYETTE MAIN BOARD/CHASSIS HARDWARE SPECIFICATION	55
**IP RATING (INGRESS PROTECTION)	56
MECHANICAL (SHOCK, VIBE) / ENVIRONMENTAL TESTING/SAFETY-MSDS (HAZARDOUS MATERIAL)	57
CHASSIS DIMENSIONS/CORRECT WIDTH	57
CHASSIS/TOP COVER SCREWS	57
1200-1000-0709 (EMPTY OPTION BAY SLOT COVERS)	58

ENVIRONMENTAL INFO (MERCURY, LEAD, ASBESTOS, PLASTICS) / HAZARDOUS MATERIAL (RB MATERIAL)	59
CONFLICT MINERALS REPORT	59
SHOCK/VIBE (MIL-STD-810F)	61
***TELCORDIA GR-63-CORE (NEBS EARTHQUAKE/SEISMIC-RELATED ENCLOSURES)	63
CCATS NUMBER FOR SECURESYNC	63
ECAT DS (ECATS) NUMBER FOR SECURESYNC	63
1200 SECURESYNC MODEL NUMBERING SCHEME	64
ENTERPRISE-LEVEL NETWORK MONITORING TOOLS (NMS)/ NRPE (SUCH AS NAGIOS, ZABBIS CACTI, SPLUNK INTEGRATION, QRADAR, ETC, XI EPOCH BY NUTANIX)	64
BOMGAR/LIEBERMAN SOFTWARE (AKA "LIEBERMAN TOOL", "LIEBSoft") PRIVILEGED ACCESS MANAGEMENT (PAM)	69
VERITAS NETBACKUP ("OS NETBACKUP")	70
FALSE ALERTS DUE TO NMS/NNMI BEING ENABLED IN THE SNMP MANAGER	71
ETHERNET MONITOR PAGE AND GRAPHS	73
CPU FREE MEMORY AND CPU USAGE/UTILIZATION (AND SYSTEM MONITOR PAGE)	74
READING THE CPU USAGE (ETX MODULE - "OUTER CPU")	78
REPORTS OF HIGH CPU USAGE (SPIKES IN CPU USAGE OR CONSTANT HIGH CPU USAGE)	80
SECURESYNC'S GENTOO OPERATING SYSTEM (OS) - SOFTWARE LICENSES/LICENSING	83
KERNEL TRACEBACK	85
CAD/3D DRAWINGS	87
KRAMDEN TIMING SYSTEM (KTS)	88
**INDICATIONS OF KTS NOT RUNNING	90
NETWORK PROCESSOR SOFTWARE (NPS) (MAIN SOFTWARE VERSIONS)	91
SECURESYNC ANCILLARY KITS, (ANC KITS/RACK EARS/BRACKETS, MANUAL CD, ETC)	93
MANUAL CDs	93
RACK-MOUNTING BRACKETS/RACK EARS/HANDLES/CHASSIS MATERIAL	93
RACK EARS/HANDLES/MOUNTING BRACKETS	96
1200-1000-0704: RUGGED ANCILLARY KIT (REAR SUPPORT BRACKETS AND AC POWER CORD SUPPORT)	99
FREQUENTLY ASKED QUESTIONS (FAQs)	103
FUSES/GROUNDING / INPUT POWER (AC AND DC) / CURRENT	104
GROUNDING	106
INPUT POWER	107
**POWER MONITOR / ALARMS / TRAPS	107
POWER INTERRUPTION TOLERANCE: UPS BACKUP TO AC INPUT FOR SECURESYNCS/9400s	114
LEAKAGE CURRENT (CURRENT LEAKAGE)	125
** (PS06R-2Z1M-DT01) AVAILABLE AC TO 24VDC CONVERTER FOR DUAL AC INPUT POWER	126
**HUMIDITY/POWER/BTU SPECS (HEAT DISSIPATION)	129
** AIRFLOW REQUIREMENTS/COOLING FAN/ TEMPERATURES	130
TEMPERATURE-OVER-TIME GRAPH (MANAGEMENT -> DISCIPLINING PAGE)	152
LITHIUM COIN CELL BATTERY (OR BATTERIES) THAT MAY BE INSTALLED / BATTERY CHANGE INTERVALS/ SHELF LIFE	155
MAIN PCB BOARD/FLASH MEMORY	155
ETX MODULE/ BIOS/ CF CARD/ RTC (REAL TIME CLOCK) / KERNEL TIME AT BOOT-UP/ RTC COIN CELL BATTERY / SHELF LIFE	156
ETX MODULE (SBC- SINGLE BOARD COMPUTER)	156
**INDICATIONS OF A POTENTIAL ETX MODULE FAILING OR ISSUE WITH THE CF CARD:	163
RTC COIN CELL LITHIUM BATTERY (BR3032)	165
ALUMINUM CAPACITORS IN SECURESYNC	169
COMPACT FLASH CARDS (CF CARDS)	170
CF CARD'S WRITES AND ERASES COUNTER DEPLETING	172
**GRUB ERRORS/INDICATIONS OF A FAILING CF CARD	178
***SENDING A REPLACEMENT CF CARD TO A CUSTOMER/REPLACING CF CARD IN THE FIELD	180
REPORT OF CF CARD/MEMORY STATUS	181
RTC (REAL TIME CLOCK) / LINUX KERNEL TIME	182
SITE ACCEPTANCE TESTING / PERFORMANCE TESTING	186
SECURESYNC OPTIONS	187
OPTIONS/LICENSE FILES AVAILABLE FOR SECURESYNC (BESIDES OPTION CARDS)	187
GENERATING/INSTALLING LICENSE FILES	187
DELETING INSTALLED OPTION LICENSES:	188
1223-SS00-OFS1: ("LAF GPI TIMESTAMPER OPTION") GENERAL PURPOSE INPUT TIME STAMPING	189

(OPT-IDM) (FKA "OPT-BSH) "SECURESYNC INTERFERENCE DETECTION SUITE OPTION" (FKA BROADSHIELD) TALEN-X /EMBEDDED BROADSHIELD INTERFERENCE AND SPOOFING DETECTION SOFTWARE	189
MONITORING BROADSHIELD / ASSOCIATED MAJOR ALARM	204
**SS-OPT-SKY (OPT-SKY/SKYLIGHT): SKYLIGHT OPTION (INDOOR GPS SYSTEM)	217
***DESIRE TO UPDATE SKYLIGHT PHASE 1 (4.7L SOFTWARE) TO SKYLIGHT PHASE 2 TO ALLOW UPDATING TO CURRENT (AND FUTURE) VERSIONS OF SOFTWARE	219
**SKYLIGHT ANTENNA (1213-0000-0600)	220
SKYLIGHT WEB BROWSER/OPERATION	229
A-GPS/A-GNSS CLIENT/SERVER (AGPS/ASSISTED GPS/ ASSISTED-GPS/ASSISTED GNSS)	229
**{SS-OPT-AGP} A-GPS /AGNSS RINEX SERVER OPTION (GPSRINEXD)	234
**{SS OPT-SKY} SKYLIGHT OPTION	237
REPLACING DISCONTINUED RAPCO MODELS 1804/2804 WITH SECURESYNC	238
**SS-OPT-TKL TIMEKEEPER OPTIONS FOR NTP/PTP	238
SPECIAL SOFTWARE PATCHES / SPECIALS FOR SECURESYNC	239
SPECIALS/PROTOTYPES	243
OPTION CARDS	256
API CALLS FOR OPTION CARDS/SLOTS	256
**SLOT NUMBERS	256
SYSTEM MEMORY (SECURESYNC AND OPTION CARDS) / SANITIZATION/	258
**GPS RECEIVER MEMORY AND CF CARD/SYSTEM MEMORY IN SECURESYNC	258
**CERTIFICATE OF VOLATILITY (COV)/ LETTER OF VOLATILITY (LOV)	258
**ETX MICROPROCESSOR MEMORY	260
MODEL AND SERIAL NUMBER	262
REPROGRAMMING MODEL NUMBER (POWER/OSCILLATOR/RECEIVER) OR SERIAL NUMBER	263
**SECURESYNC CALIBRATION SERVICE	265
SOFTWARE VERSION/SOFTWARE UPDATE/SOFTWARE DOWNGRADE/RESTORE TO DEFAULTS	266
**SOFTWARE LICENSES/EULAs FOR THE SECURESYNC'S INTERNAL FIRMWARE	267
**PERFORMING SOFTWARE UPDATES/STEP UPDATE REQUIREMENTS	267
SPECIFIC SOFTWARE VERSION NOTES (INFO NOT NECESSARILY IN RELEASE NOTES)	268
CLEANER FILE/SOFTWARE UPDATES/UPGRADE ISSUES	268
RESTRICTIONS ON/RECOMMENDATIONS FOR PERFORMING SOFTWARE DOWNGRADES TO EARLIER SOFTWARE VERSIONS	274
SOFTWARE UPLOAD FAILURES (FAILURE UPLOADING THE UPGRADE FILE INTO THE SERVER)	275
**SOFTWARE UPGRADE FAILURES (FAILURES AFTER STARTING THE UPDATE PROCESS)	276
**LICENSE FILES (FOR PURCHASED OPTIONS)	285
***SC037 ("TRADE AND INDUSTRY DEPARTMENT CRYPTOGRAPHY QUESTIONAIRE")/BLOWFISH	286
SYSTEM INITIALIZATION AFTER EACH BOOT-UP	286
THIRD-PARTY SOFTWARE PACKAGES USED/NOT USED IN SECURESYNCS	287
FRONT PANEL / KEYPAD	288
**FRONT PANEL LCD / LED TIME DISPLAY / KEYPAD	289
LCD DISPLAY COMPONENT	289
API CALLS ASSOCIATED WITH FRONT PANEL DISPLAY	290
***CONFIGURE FRONT PANEL LED CLOCK (AND CLOCK IN WEB BROWSER) TO DISPLAY LOCAL TIME	291
***CONFIGURE/DISPLAY NETWORK SETTINGS USING THE FRONT PANEL KEYPAD/LCD	292
CONFIGURE ETH0 VIA KEYPAD WITH NO NETWORK CABLES CONNECTED TO THE UNIT (0.0.0.0 WILL BE DISPLAYED)	293
FRONT PANEL MENUS THAT CAN BE DISPLAYED IN LCD WINDOW	296
LCD/KEYPAD	297
KEYPAD FROZEN/NOT RESPONDING OR VERY SLUGGISH	298
**FRONT PANEL KEYPAD LOCK/UNLOCK	298
**FRONT PANEL STATUS LEDs (AC AND DC POWER MONITORING)	300
***ABILITY TO MASK/OVERRIDE THE POWER LED/POWER ALARM (IF BACKUP POWER IS NOT CONNECTED)	302
KNOWN ISSUES/CONDITIONS ASSOCIATED WITH FRONT PANEL LCD/ LED TIME DISPLAY/FRONT PANEL RIBBON CABLE	304
**OUT-OF-BAND MANAGEMENT/FRONT PANEL DB9F SERIAL CONSOLE SETUP PORT	309
CLI (COMMAND LINE INTERFACE)	313
"vi" TEXT FILE VIEWER/EDITOR	313
ALTERNATE INTERFACE TO USING THE LIMITED CLI COMMANDS	313
**SECURITY WITH THE CLI INTERFACE (ABILITY TO CONNECT OUT USING FTP, SCP/SFTP, ETC)	313
"su" COMMAND TO SWITCH USERS (SUCH AS SU SPFACTORY) (FOR INTERNAL USE ONLY)	314
AVAILABLE CLI CALLS (API CALLS)	315

***TROUBLESHOOTING ISSUES WITH CLI COMMANDS	315
*SPECIFIC AVAILABLE CLI COMMANDS/API CALLS/ FUNCTIONS	318
SYSTEM STATUS COMMANDS	319
HEALTHCHECK.SH CLI COMMAND TO CHECK THE CF CARD HEALTH	320
MANIFEST: CLI COMMAND TO DISPLAY ENTIRE MANIFEST.LOG (V5.7.1 AND ABOVE ONLY)	321
CLI COMMAND FOR KTS INITIALIZATION TEST RESULTS (IN_GetSTATUS 0)	321
**CLI COMMANDS ENABLE/DISABLE, DISPLAY, CONFIGURE THE ETHERNET PORTS (DNS, DHCP, IP ADDRESS, SUBNET MASK, STATIC ROUTES)	323
ENABLE/DISABLE NETWORK INTERFACES VIA CLI COMMANDS (PORTSTATE/PORTSET COMMANDS)	323
ENABLE/DISABLE LINK NEGOTIATION AND ABILITY TO HARD-SET PORT SETTINGS (V5.7.3/5.8.0 AND ABOVE ONLY)	324
DNS SERVERS (PRIMARY AND SECONDARY DNS SERVERS) ("RESOLV.CONF" FILE)/LLMNR	325
***ASSIGNING NETWORK SETTINGS	328
READING/ MANUALLY SETTING DATE AND TIME (VIA CLI OR BROWSER)	331
GETTEMP: OBTAIN OSCILLATOR, BOARD AND CPU TEMPERATURE READINGS VIA CLI (APPLICABLE TO VERSIONS 5.4.5 AND ABOVE ONLY)	336
**VERSION COMMANDS (LINUX OS AND SPECTRACOM SOFTWARE)	336
GNU BASH	339
"STR_" ERROR MESSAGES IN SYSTEM LOG (VERSIONS 5.8.0 THROUGH 5.8.4 ONLY)	339
**REVIEWING/SAVING/DELETING LOGS VIA CLI INTERFACE	339
SAVED LOG BUNDLE WAY TOO SMALL (ONLY ~15KB) WHEN DOWNLOADED USING BROWSER AND ONLY CONTAINS HTML CODE WHEN OPENED	341
DESIRE TO AUTOMATICALLY DELETE THE LOGS ON A PERIODIC SCHEDULE	342
TESTING SNMP TRAPS AND EMAIL ALERTS (TESTEVENT AND SENDTRAP COMMANDS)	342
SYSTEM START-UP SEQUENCE/BOOT-UP AND INTIAL EFFECTS OF SIGNATURE CONTROL ON OUTPUTS	343
**CONFIGS/CONFIGURATIONS (SAVE CONFIGS /BACKUP AND RESTORE CONFIGS/CLEAN CONFIGS)	345
SECURITY CONSIDERATIONS/DEFAULT AND RECOMMENDED CONFIGURATIONS	345
**SAVE/BACKUP CONFIGS/RESTORE CONFIGS/SAVECONF COMMAND (CONFIGURATION FILES)	347
ETC/MOTD FILE (CONFIG FILES FOR SOFTWARE VERSIONS 5.0.0 AND ABOVE)	350
**CLEAN COMMAND (RESET LOGS AND CONFIGS)	356
DESIRE TO PERFORM SCRIPT/SCRIPTING FOR AUTOMATING THE CONFIG BACKUP PROCESS	356
BREAKDOWN OF ALL THE VARIOUS CONFIG FILES	365
**CLI COMMANDS TO DISPLAY / CONFIGURE / DISABLE THE ETHERNET PORTS (DNS, DHCP, IP ADDRESS, SUBNET MASK, STATIC ROUTES)	372
***ASSIGNING NETWORK SETTINGS	375
"FREE", "FREE MEM" (FREE -M) AND "CAT/PROC/MEMINFO" MEMORY COMMANDS	380
SYSTEM "UPTIME"	380
COMMAND TO RESET THE NETWORK ACCESS TABLE	380
MANUALLY DELETE AN UPDATE FILE (IF CAN'T DELETE IT VIA THE BROWSER)	381
ABILITY TO PERFORM SOFTWARE UPDATES VIA CLI INTERFACE (FOR SCRIPTING UPDATES)	382
BASE 10MHZ OUTPUT ENABLE / DISABLE OUTPUT CONTROL	382
COMMANDS TO ZEROIZE SAASM RECEIVER (WHEN INSTALLED)	383
CF CARD MEMORY USAGE / "DU" COMMAND	384
ENABLE/DISABLE HTTPS	400
SERVICES	402
TELNET/SSH (OPENSSSH)	402
VULNERABILITY SCAN FINDINGS ASSOCIATED WITH SSH	404
***VIEW THE OPENSSSH CONFIG FILE (SSHD_CONFIG)	405
TROUBLESHOOTING TELNET/SSH ISSUES	413
FTP AND SFTP/SCP (SECURE COPY PROGRAM)	416
**TCPFORWARDING (TCP FORWARDING)	416
USER RIGHTS/PERMISSIONS	416
SECURITY ALGORITHMS (SUCH AS RC4)	417
SERVICES/PROCESSES/DAEMONS WHICH MAY BE RUNNING	418
LIST OF VARIOUS DAEMONS/SERVICES/PROCESSES WHICH MAY BE ENABLED/RUNNING IN THE UNIT	418
CONTROLLING SERVICES AS SPFACTORY (INTERNAL USE ONLY)	419
NETWORK RELATED (NETWORK SETTINGS/DNS/PORT ENABLING)	422
NETWORK DISCOVERY/NETWORK AUTO DISCOVERY/AUTO-DISCOVERY	422
MANAGEMENT -> NETWORK SETUP PAGE (FOR ETH0, ETH1, ETH2, ETH3)	422
DISPLAY NETWORK (UDP/TCP) NETWORK PORTS OPEN/NETWORK PORT ASSIGNMENTS (SUCH AS PORT 123 IS FOR NTP)	423
NETSTAT COMMANDS	423
"UNEXPECTED" NETWORK PORTS BEING REPORTED AS OPEN/LISTENING	424

**PORT SPEEDS/DUPLEX SELECTIONS	425
(APPLICABLE TO V5.9.4) PERIODIC ETH0 LATENCIES (SUCH AS DELAYS IN PING, NTP OFFSET SPIKES)	426
10/HALF CAN CAUSE ETH0/ETX LOCK-UPS (VERSIONS 5.4.1 AND BELOW)	426
UNIT LOCKUPS AND NO/LOSSES OF NETWORK CONNECTIVITY BETWEEN ETH0 AND A SWITCH/UNLESS BOTH DEVICES ARE HARD-SET (INSTEAD OF AUTO-NEGOTIATE)	427
**DESIRE TO ENABLE/DISABLE THE GIGABIT INTERFACES (ETH1, ETH2 AND/OR ETH3)	427
**DESIRE TO DISPLAY PORT STATE OF ALL ETHERNET PORTS (PORT UP, PORT DOWN, CABLE UNPLUGGED)	430
DNS SERVERS SETTINGS (PRIMARY AND SECONDARY DNS SERVERS)	431
**DNS HOST NAME/ FULLY QUALIFIED DOMAIN NAME (FQDN)/(HOSTNAME/HOST NAME)	433
**ARPS / ARP CACHING	437
**TCP CONNECTION/TCP SESSION TIMEOUTS	437
HALF-OPEN TCP SESSIONS	438
** NETWORK ISOLATION/NETWORK SECURITY/FIPS COMPLIANCY	439
***IEEE 802.3	439
**USB CONNECTOR/ ETHERNET PORT (ETH0- ETH3) STATUS LEDs / CONFIGURATION	440
IP ADDRESS CONFIGURATION/IPSETSD	441
DHCPv4/DHCPv6	441
DHCLIENT ("STATIC LEASE" DEFAULT IP ADDRESSES FOR THE ETHERNET INTERFACES)	441
ETHERNET BONDING (TWO IP ADDRESSES ASSIGNED TO SAME PORT) / LINK AGGREGATION	446
NETMASK SETTINGS	446
AUTO-MDIX	447
**TROUBLESHOOTING ISSUES WITH NETWORK CONFIGURATION/OPERATION	449
IPTABLES (DESIRE TO FILTER PACKETS FROM GETTING INTO THE SECURESYNC/9400s)	450
**IPv6 ADDRESSES (SUCH AS SLAAC ADDRESS / LINK-LOCAL ADDRESS. GLOBAL UNICAST ADDRESS)	455
**MAIN DEFAULT PORT/MAIN DEFAULT GATEWAY ADDRESS	456
** INDIVIDUAL GATEWAY ADDRESSES (IPv4/IPv6) FOR EACH INTERFACE	459
RFC-2462 (RFC 2462): IPv6 SLAAC ADDRESSES (STATELESS ADDRESS AUTOCONFIGURATION FOR IPv6)	467
STATIC ROUTES/ DEFAULT ROUTES/STATIC ROUTING/ ROUTING TABLES	470
IPv6 STATIC ROUTES	477
**NETWORK TROUBLESHOOTING IN SECURESYNC (TCPDUMP, PING, ARP, TRACEROUTE/TRACEPATH, ETC)	480
TCPDUMP (WIRESHARK FOR LINUX)	480
AVAILABLE CLI COMMANDS FOR TROUBLESHOOTING NETWORK ISSUES (PING, TRACEROUTE, DIG, ETC)	489
DIG: (DOMAIN INFORMATION GROPER)	494
NETSTAT AND SS COMMANDS (PORTSCAN TO SEE WHICH PORTS ARE OPEN)	495
LOOPBACK INTERFACE/LOGICAL INTERFACE	496
SAMBA SOFTWARE	496
NESSUS CREDENTIALLED SCANS/VULNERABILITY SCANS	497
CREDENTIALLED VULNERABILITY SCANS/ELEVATED CREDENTIALLED SCANS	497
***USER ACCOUNTS AND PASSWORDS (ROOT/SPADMIN/SPFACTORY/SPUI ETC)	498
USER ACCOUNTS / PERMISSIONS	505
CREATING NEW ACCOUNTS/EDITING ACCOUNTS	505
ACCOUNT PASSWORDS	511
***/ETC/SHADOW FILE (LINUX PASSWORD FILE)	511
RESET THE SPADMIN ACCOUNT PASSWORD	514
RETRIEVING/CHANGING USER ACCOUNT PASSWORDS	516
**RETRIEVING UNKNOWN ACCOUNT PASSWORD	516
"CHANGE MY PASSWORD" BUTTON (NEWER BLACK/SILVER BROWSER ONLY)	518
"PASSWORD SECURITY" (AVAILABLE MINIMUM PASSWORD RULES/REQUIREMENTS THAT CAN BE ENFORCED, IF DESIRED)	520
ROOT AND SPFACTORY ACCOUNTS	525
PASSWORD RE-USE/PASSWORD HISTORY	526
WEB BROWSER (HTTP/HTTPS) SSL / ENHANCED SECURITY / LOGIN ACCOUNTS / BANNER	529
NETWORK PORT NUMBERS FOR THE WEB BROWSERS (443 FOR HTTP, 80 FOR HTTPS, AND 8080)	529
***ACCESSING THE CLASSIC INTERFACE BROWSER	529
***ENABLE/DISABLE THE CLASSIC INTERFACE BROWSER VIA CLI (v5.5.0 THRU 5.8.9)	529
***QUAGGA ACCOUNT DISPLAYED IN CLASSIC INTERFACE	530
FAILED PASSWORD ATTEMPTS/LOCK PLACED ON BROWSER (AND CLI) AFTER FAILED BROWSER LOGINS	531
**PC BROWSER REQUIREMENTS	531
***JAVA TO RUN JAVASCRIPT	531

***ADOBE FLASH	532
***PHP	532
***HOME PAGE OF THE NEWER BROWSER	533
***CUSTOMIZATION OF THE NEWER BROWSER	533
***PRODUCT REGISTRATION REMINDER / REGISTER YOUR PRODUCT	534
***DESIRE TO CREATE SCRIPTS FOR THE WEB BROWSER INTERFACE	534
CORRUPT BLACK/CHARCOAL BROWSER DISPLAY (LOOKS LIKE AN "OUTLINE" FORMAT WITH JUST WORDS)	534
*COOKIES FOR CLASSIC/NEWER BROWSERS	536
"HTTPONLY" AND "SECURE CONNECTIONS ONLY" / "ENCRYPTED CONNECTIONS ONLY" COOKIES	537
DESIRE TO DISABLE APACHE CBC CIPHERS	538
CONCURRENT SESSIONS (BROWSER AND CLI INTERFACE)	538
INVALIDATING SESSION IDENTIFIERS/SESSION INVALIDATED	538
*SUPPORTED/UNSUPPORTED WEB BROWSERS AND BROWSER VERSIONS	539
SIGNATURE ALGORITHMS (SUCH AS SHA1, SHA256 AND MD5)	539
INTERNET EXPLORER VERSIONS SUCH AS IE 11 NOT LOGGING IN, WITH NO ERROR MESSAGES BEING DISPLAYED	541
**OPENSSL VERSION INSTALLED	543
DETERMINING IF APACHE WEB BROWSER IS RUNNING	543
*RESTART HTTP/HTTPS INSTEAD OF REBOOTING THE UNIT (HTTPS RELOAD COMMAND)	543
GRACEFUL RESTART OF APACHE BROWSER (GRACEFUL RESTART REQUESTED, DOING RESTART)	544
MONITORING SERVICES	545
**WATCHDOG (APPLICABLE TO VERSIONS 5.8.9 AND ABOVE, JUNE 2020)	545
WEB BROWSER TIME DISPLAY (UPPER RIGHT CORNER OF THE BROWSER)	546
TROUBLESHOOTING/KNOWN ISSUES WITH LOCAL TIME ERROR IN WEB BROWSER	547
HTTP / HSTS (HTTP STRICT TRANSPORT SECURITY)	548
HSTS SETUP/CONFIGURATION (APPLICABLE TO VERSIONS 5.9.4 AND ABOVE ONLY)	549
**HTTPS/SSL CERTIFICATES (HTTPS CERTIFICATES)	552
ROOT CERTIFICATE/INTERMEDIATE SSL CERTIFICATES (CHAIN CERTIFICATES)	553
ISSUES WITH CREATING/INSTALLING A NEW SSL CERTIFICATE (HTTPS CERTIFICATE)	565
"ACCOUNT LOCKED DUE TO XX FAILURES": LIMIT NUMBER OF WEB BROWSER/SSH LOGIN ATTEMPTS/RE-TRIES (ENTERING INCORRECT PASSWORD SEVERAL TIMES IN A ROW)	568
**APACHE WEB BROWSER/GENERAL LOCK-UP TROUBLESHOOTING (ERROR MESSAGES DISPLAYED/ABNORMAL WEB BROWSER OPERATION, SLUGGISH BROWSER, ETC)	571
**INDICATIONS OF KTS (KRAMDEN TIMING SYSTEM) NOT RUNNING	571
***REST API INTERFACE/POSTMAN (ALTERNATE TO USING THE STANDARD WEB BROWSER OR CLI)	571
FIND OUT WHAT WEB BROWSER (AND ITS VERSION) THEY ARE USING ON THE PC (SUCH AS IE11, FIREFOX, ETC).	581
SPECIFIC EXAMPLES WHERE REST API CAN BE USED	590
PYTHON SCRIPTS/SCRIPTING USING REST API	600
***WEB BROWSER IDLE LOGIN TIMEOUT (LOGIN TIME-OUT AFTER NO ACTIVITY)	602
APACHE WEB SERVER IN SECURESYNC	604
LOG ENTRIES FOR UNSUCCESSFUL/SUCCESSFUL BROWSER LOGINS	605
(LAFAYETTE DATABASE) MYSQL/SQLITE DATABASES AND DB BROWSER	606
ORACLE DATABASE (NOT USED/APPLICABLE TO SECURESYNCS/9400s)	611
APACHE STRUTS AND APACHE TOMCAT SERVER	612
**WEB BROWSER CAN'T OPEN (CAN'T LOGIN AT THE LOGIN PROMPT OR PROMPT NOT DISPLAYED) YET TELNET AND/OR SSH IS WORKING	612
SUMMARY TO POTENTIALLY FIX ISSUES WITH THE APACHE BROWSER	613
***NO ERROR MESSAGES DISPLAYED WHEN TRYING TO LOGIN (STAYS AT LOGIN SCREEN)	616
***ERROR MESSAGES DISPLAYED WHEN TRYING TO LOGIN/NAVIGATE BETWEEN BROWSER PAGES	617
DU COMMAND (USE IF THE CF CARD IS QUITE OR COMPLETELY FULL)	625
*INTERNET EXPLORER NOT DISPLAYING THE GEAR ICONS ON THE WEB PAGES	625
LOGIN BANNERS	626
GLIBC	629
OPENSSL (SECURE SOCKET LAYER) /TLS-SSL FOR ENCRYPTION (AND HTTPD.CONF FILE)/SECURITY LEVEL	630
***TLS (TRANSPORT LAYER SECURITY) SUCH AS TLS 1.0, 1.1, 1.2 ETC	630
SSL CIPHER SUITES (CBC CIPHERS) / MAC ALGORITHMS	632
*AES (ADVANCED ENCRYPTION STANDARD)	639
**MTU (MAXIMUM TRANSMISSION UNIT)	639
**NETWORK PORTS/MANAGEMENT/NETWORK ACCESS RESTRICTION (ACCESS CONTROL)	640

COMMAND TO RESET THE NETWORK ACCESS TABLE (UNRESTRICT)	641
**VLANs/VLAN TAGGING (IEEE 802.1Q)	644
ACS / AAA / SECURE ACS (CISCO STANDARDS) PROTOCOLS / ENVIRONMENTS.	645
RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE)	647
***OUR RADIUS SERVER IN ROCHESTER	648
GENERAL INFO ON RADIUS	649
RADIUS AUTHENTICATION	649
RADIUS EXTENSIONS FOR OPENRADIUS (RFC 2869)	649
**RADIUS WITH IPV6 ADDRESSES	650
***RADIUS VENDOR-SPECIFIC ATTRIBUTES (VENDOR SPECIFIC ATTRIBUTES) (VSAs)-VENDOR CODE/VENDOR ID	653
***RADIUS CONFIGURATION	656
RADIUS KNOWN ISSUES/TROUBLESHOOTING	658
RADIUS NOT WORKING ON A UNIT	664
***NAS (NETWORK ACCESS SERVER)	667
***PERMISSIONS ASSIGNED TO RADIUS ACCOUNTS	667
LDAP	669
OUR LDAP SERVER	669
LDAP CONFIGURATION:	672
***LOGIN ACCESS LEVELS (PERMISSIONS/RIGHTS)	689
***KNOWN ISSUES WITH OPENLDAP/ACTIVE DIRECTORY	697
***TROUBLESHOOTING LDAP	701
KNOWN ISSUES WITH LDAP	707
TACACS + (REMOTE AUTHENTICATION)	709
TACACS AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)	709
CISCO ISE (IDENTITY SERVICES ENGINE)	710
CONFIGURATION OF TACACS + IN 1200 SECURESYNCS / TACACS CONFIG FILES	713
TACACS ATTRIBUTE INFO/ATTRIBUTE-VALUE (AV) PAIRS	714
TACACS OPERATION	718
TROUBLESHOOTING ISSUES WITH TACACS LOGIN/KNOWN ISSUES	726
IPASS	733
HALT/SHUTDOWN (SOFTWARE ONLY) /SYSTEM REBOOT/POWER CYCLE	734
REPORT OF SECURESYNC APPEARING TO HAVE REBOOTED ITSELF	737
LINUX PREEMPT/PREEMPTION (POTENTIAL CAUSE OF LOCK-UPS/ SYSTEM HANGING??)	737
**PARALLEL REDUNDANCY PROTOCOL (PRP)	738
**IPSEC (IP SECURITY)	738
TIME MANAGEMENT (SYSTEM TIME, GPS/TAI OFFSETS, LOCAL CLOCKS)	739
**SYSTEM TIME/YEAR AND SYSTEM TIMESCALE	739
SYSTEM YEAR / "SET YEAR ONLY" CHECKBOX/FIELD	741
**GPS OFFSET (ANTENNA CABLE DELAY/ACD) (AKA GNSS RECEIVER OFFSET)	744
**"GPS TO UTC OFFSET" (NUMBER OF LEAP SECONDS)	745
LEAP YEARS (LEAP DAYS)/FEBRUARY 29 TH	745
**LEAP SECOND INSERTION	746
**LOCAL SYSTEM CLOCKS (LOCAL CLOCK)	758
INPUT REFERENCES / REFERENCE PRIORITY TABLE/ REFERENCE MONITOR/TIME SYNC / HOLDOVER	762
MANAGEMENT -> REFERENCE PRIORITY PAGE	763
**INPUT REFERENCE MONITORING (5.4.5 AND ABOVE)	764
**SMART REFERENCE QUALITY MONITORING/REFERENCE 1PPS VALIDATION/YELLOW PPS REFERENCE STATUS INDICATOR	770
**INPUT "REFERENCE STATUS" TABLE	777
SWITCHING FROM ONE INPUT REFERENCE TO ANOTHER	778
TIME TO SYNCHRONIZE SYSTEM TIME ONCE AN INPUT REFERENCE IS PRESENT AND VALID	778
NTP INPUT	779
** "TIME RESET" WHEN NTP FIRST STARTS-UP	779
NTP/EXTERNAL PPS INPUT	779
"ACCURACY NOT DETERMINED" (REPORTED TOP-LEFT CORNER OF HOME PAGE, UNDER "REFERENCE" FIELD)	781
DSCP VALUES FOR NTP	783
***ISSUES WITH NTP STRATUM SYNCHRONIZATION	785
PTP INPUT	787

IRIG INPUT	787
**TIME SYNCHRONIZATION FOR SECURE NETWORKS USING FIBER	787
USING A DAGR AS AN INPUT REFERENCE TO SYNC SECURESYNC	787
HAVEQUICK/STANAG INPUT	787
ASCII INPUT	787
MANUALLY SETTING THE SYSTEM TIME (USER/USER "SELF" MODE)	787
ENABLE BATTERY BACKED TIME (TIME SYNC IMMEDIATELY UPON BOOT-UP)	792
LOCAL SYSTEM REFERENCE (SELF REFERENCE)	793
NTP OPERATION WHILE IN USER/USER MODE	793
NTP STEP THRESHOLD (NTP'S REFERENCE TIME CHANGE LIMITS)/ NTPMOND RESTARTING NTPD	794
STL *(SATELLES) "RESILIENT PNT" INPUT OPTION CARD (OPTION CARDS 1204-3E AND 1204-3D)	796
GPS/GNSS (GNSS 0) INPUT	797
GPS/GLONASS/QZSS SAASM GPS INPUT REFERENCE- GPS RECEIVER OPERATION /MOBILE (DYNAMIC) MODE OPERATION/SAASM	797
DESIRE TO ADD A GNSS RECEIVER TO THE SECURESYNC/9400 IN THE FIELD (AFTER INITIAL PURCHASE)	797
DOWNLOADING/QUERYING GNSS 0 DATA VIA CLI INTERFACE, .CSV FILE OR REST API	798
GPS INFO ("GR_" CLI COMMANDS)	799
**OUTPUT GPS POSITION INFORMATION (LATITUDE, LONGITUDE, ALTITUDE)	801
ICD-GPS-153C MESSAGES (GROUND SPEED, HEADING)	803
GPS RECEPTION ISSUES/GPS JAMMING	805
GPS/GNSS RECEIVER AND ANTENNA (SUCH AS MODEL 8230) IS "RECEIVE-ONLY" (IT DOESN'T TRANSMIT)	806
STORAGE OF ALMANAC AND EPHEMERIS DATA/A-GPS SERVER LICENSE	806
GPS/GNSS RECEIVER MODELS	808
DETERMING WHICH MODEL RECEIVER IS INSTALLED AND ITS CURRENT FIRMWARE VERSION	808
UBLOX M8T, TRIMBLE RES-SMT-GG AND TRIMBLE RES-T	809
**DESIRE TO BLACKLIST (MASK/UNMASK) A SATELLITE FROM BEING RECEIVED BY A TRIMBLE RES-SMT-GG RECEIVER	809
U-BLOX MODEL M8T RECEIVERS	810
"GPS0 UBX MESSAGE RECEIVE CHECKSUM ERROR"/ "GPS0 UBX MESSAGE RECEIVE BUFFER OVERFLOW	812
TRIMBLE RES-SMT-GG GNSS RECEIVERS	815
RES-SMT-GG FIRMWARE VERSIONS AND KNOWN ISSUES	815
GPS-GLONASS-BEIDOU-QZSS-GALILEO SATELLITE CONSTELLATION / NUMBER OF SATELLITES BEING TRACKED	819
**GR_GETSATDATA 0 0 CLI COMMAND (UNDOCUMENTED COMMAND)	826
***GNSS SATELLITES/SIGNAL STRENGTHS (SIGNAL TO NOISE) GRAPHS	827
**GPS RECEPTION/RECEIVER TROUBLESHOOTING/ISSUES WITH GPS RECEPTION	830
BENT CENTER PLATE ON REAR PANEL TYPE N GPS INPUT CONNECTOR	831
**GPS ANTENNA PROBLEM ALARM	831
MOBILE (CONTINUOUS) MODE AND SINGLE SATELLITE MODE	833
**OPERATIONAL SPEED AND ALTITUDE LIMITATIONS	833
DEGRADATION OF TIMING/POSITIONAL ACCURACIES WHILE IN MOBILE MODE (CONTINUOUS MODE)	833
"REC MODE ERROR: ERROR 12 (KTSAL)	835
SINGLE SATELLITE MODE:	839
RECEIVER RESET/RESET GNSS RECEIVER	840
USER-DEFINED MINIMUM SATELLITES ALARMS/TRAPS	841
GPSD (GPS SERVICE DAEMON)	842
SAASM GPS RECEIVERS (ROCKWELL COLLINS GB-GRAM /TRIMBLE FORCE-22)	843
SAASM GPS RECEIVER OPERATION	844
DEPT OF DEFENSE FORM DD-1494 (DD1494 FOR SAASM)	844
TROUBLESHOOTING/KNOWN ISSUES WITH SAASM RECIEVERS	847
M-CODE (M CODE) RECEIVER/CAPABILITIES	848
SBAS	848
OPT-SEM (OPTION SAASM MODULATION)/ TIME MARK DATA MESSAGE (ID 3)	848
T1 AND E1 INPUT	849
**MSF/WWVB/DCF77	849
**T1/E1 AND AFNOR INPUT TIME REFERENCES	851
**EXTERNAL 1PPS INPUT (EPP0)	852
"FREQUENCY 0" (FREQ 0) EXTERNAL INPUT FREQUENCY (SUCH AS 10 MHZ INPUT)	852
*REFERENCE STATUS TABLE	853
**TIME SYNC / HOLDOVER MODE	855

**LOCAL INTERFERENCE, GPS JAMMING AND GPS SPOOFING	859
OSCILLATORS/ DISCIPLINING TO 1PPS INPUT REFERENCE/TFOM/1PPS PHASE ERROR	860
**TYPES OF AVAILABLE OSCILLATORS/INSTALLED OSCILLATOR TYPE	860
WHICH TYPE OSCILLATOR IS INSTALLED?	860
TYPES OF OSCILLATORS THAT CAN BE INSTALLED	860
LOCK STATUS FOR RAYTHEON AMDR SPECIAL SECURESYNC (OUR RB OSCILLATOR LOCKING A WENZEL OCXO OSCILLATOR VERY LOW PHASE NOISE OCXO)	866
ISSUE: GLITCHES IN 10 MHZ OSCILLATOR (TYPICALLY ASSOCIATED WITH OCXO) OUTPUT CAUSES LED TIME TO STOP COUNTING UP. LCD DISPLAY IS FINE.	868
OSCILLATOR ASSOCIATED ALARMS NOT SPECIFIC TO OSCILLATOR TYPE	869
*FREQUENCY ERROR ALARM	869
**RUBIDIUM OSCILLATOR-ASSOCIATED ALARMS	871
**OSCILLATOR FREE-RUN/HOLDOVER SPECS	871
SONET/TELECOM STRATUM HIERARCHY LEVELS FOR 1544/2048 KHZ, T1/DS1 AND E1 OUTPUTS	873
HOLDOVER FOR SIMULCAST SPECS (TIME TO DRIFT 5 MICROSECONDS)	873
**OSCILLATOR WARM-UP/STABILIZATION (TIME TO WARM UP TO OPERATING TEMPERATURE)	873
**OSCILLATOR CALIBRATION (HERTZ RANGE/DAC VALUES)/RECALIBRATE CHECKBOX	875
**OSCILLATOR DISCIPLINING (RB/OCXO/TCXO)	880
***** (HST1) HOST DISCIPLINING OF OSCILLATOR WHEN NTP OR "USER SET TIME" IS THE SELECTED REFERENCE	884
API CALLS ASSOCIATED WITH HOST REFERENCE (NTP INPUT)	884
RUBIDIUM OSCILLATOR DISCIPLINING	888
OSCILLATOR 10 MHZ ACCURACY (OSCILLATOR ACCURACY WHEN LOCKED TO A REFERENCE)	895
EFFECTS OF NTP PEERING ON THE OSCILLATOR/SYSTEM PPS/1PPS OUTPUTS	895
**FRACTIONAL FREQUENCY ERROR (FFE) FOR 10 MHZ	895
1200-FAST (SPECIAL FREQUENCY ACCURACY AND STABILITY TEST FOR 10MHZ OUTPUTS)	898
*OSCILLATOR 10 MHZ ACCURACY (FREQUENCY ERROR)	899
"FREQUENCY ERROR RECALCULATED" MESSAGES IN THE OSCILLATOR LOG	901
"RB REFERENCE UNSTABLE" / "RB SYNCHRONIZED" / "RB TRACK OFF -- FREE RUN"	904
HOLDOVER MODE/ OSCILLATOR 10 MHZ FREE-RUN (OSCILLATOR STABILITY)	908
**"RB(SYNC)" DISPLAYED ON THE FRONT PANEL LCD	913
**1PPS PHASE ERROR / TFOM / MAXTFOM	915
1PPS PHASE ERROR CORRECTIONS (1PPS STEP SIZES/PERIOD BETWEEN ADJUSTMENTS)	919
TOO HIGH/HIGHER THAN EXPECTED TFOM/PHASE ERRORS	923
**RESTART TRACKING / "PHASE ERROR LIMIT" / "ALWAYS RESTART TRACKING AFTER SYNC"	924
TFOM (TIME FIGURE OF MERIT)	930
MAXTFOM (MAX TFOM / "MAXIMUM TFOM FOR SYNC")	935
**OPT-TKL (TIMEKEEPER SOFTWARE IN SECURESYNC)	940
IPV6 SUPPORT WITH PTP	941
IF THE THREE TIMEKEEPER TABS AREN'T VISIBLE AT TOP OF "TIMEKEEPER MONITORING" PAGE	942
***TIMEKEEPER SOFTWARE OPERATION	944
***SOURCECHECK	945
*** TIMEKEEPER NTP OUTPUTS/PTP OUTPUTS	950
***NTP CLIENT LISTS (TIMEKEEPER'S TIMEMAP FUNCTION VS THE NTP CLIENT LIST IN STANDARD NTP)	951
***TIMEKEEPER CONFIGS / TIMEKEEPER LOGS	952
***TIMEKEEPER STATUS MONITORING OF NTP/PTP CLIENTS AND SERVERS	953
SYSTEM ALARMS (MAJOR AND MINOR ALARMS)	956

6.

ENCY ERROR ALARM	FREQU	957
DESIRE TO MASK OR UNMASK ALARMS/EVENTS		962
**OBTAINING TIME/DATE READS (DESIRE TO READ/OBTAIN TIME REMOTELY/AUTOMATICALLY)		963
**IBM MODEL 9037 SYSPLEX TIMER (SYSPLEX1) TIME STAMPS		964
***PTP OUTPUT, IRIG OUTPUT, ASCII OUTPUT, ETC		964
IPV6 SUPPORT WITH PTP		964
**1PPS OUTPUT (ON-TIME POINT /SYSTEM 1PPS) / 1PPS GENERATION		965
EFFECTS OF NTP PEERING ON THE OSCILLATOR/SYSTEM PPS/1PPS OUTPUTS		969
**SYSTEM TIME MESSAGE DAEMON" FUNCTION (STMD) (MARKER FOR THE TIME TO NEXT 1PPS)		970
SIGNATURE CONTROL FOR VARIOUS OUTPUTS (SUCH AS IRIG, 1PPS, 10 MHZ, ETC)		978
**10 MHZ OUTPUT(S)		979

****10 MHZ PHASE ALIGNMENT TO 1PPS INPUT REFERENCE/DISCONTINUITIES BETWEEN 10MHZ VS 1PPS/1MHZ AND 5 MHZ OUTPUTS	980
****10 MHZ OUTPUT SIGNATURE CONTROL	985
***10 MHZ OUTPUT PHASE NOISE / HARMONICS/ SPURS	985
****OSCILLATOR WARM-UP TIME	990
****FREQUENCY ACCURACY ERROR MEASUREMENTS	990
**SHOW CLOCK PAGE (SYSTEM DATE/TIME DISPLAY IN THE BROWSER)	992
**SMPTE TIME CODE (LTC AND VITC)	992
LOGS/SYSLOGD	993
LOGS	1007
LOG REQUIREMENTS FOR PCI-DSS/ PCI COMPLIANCE	1007
MISSING EXPECTED LOG ENTRIES/"SEARCH" FIELD FOR THE LOGS (TOP RIGHT OF THE INDIVIDUAL LOG PAGES)	1007
REPORTING OF MODEL AND VERSION IN THE LOGS/LOG CAPTURE	1008
**ABILITY TO VIEW THE LOGS (LOG ENTRIES) WITH CLI INTERFACE	1009
**ABILITY TO DELETE THE LOGS	1009
FAQS REGARDING LOG ROTATIONS	1011
LOG CONFIGURATION/MAPPING (FACILITY AND SEVERITY CODES)	1013
****DELETING/CLEARING LOG FILES	1017
**NTPSTATS/NTP STATISTICS (LOOPSTATS, PEERSTATS, CLOCKSTATS AND SYSSTATS)	1019
**"AWK" AND "SED" FILTERS FOR LOGS	1025
**SPECIFIC LOG FILE ENTRIES	1026
CLOCKSTATS (NTPSTATS)	1036
DISCSTATS	1037
KERN.LOG	1051
NTP.LOG ENTRIES (NTP LOG ENTRIES)	1064
SYSTEM.LOG ENTRIES	1073
**TROUBLESHOOTING "OUT OF MEMORY / KILLED PROCESS" ENTRIES IN SYSTEM LOG	1073
RC.LOG (RACCOON LOG)	1097
"STR_" ERROR MESSAGES IN SYSTEM LOG (VERSIONS 5.8.0 AND ABOVE ONLY)	1111
USER.LOG ENTRIES	1123
WTMP.LOG	1124
/VAR/LOG DIRECTORY (LINUX LOGIN LOGS SUCH AS LASTLOG)	1126
CHRONY/CHRONYD	1127
NTP	1128
NTP VERSIONS IN OUR SOFTWARE	1128
NTP'S TIMESCALE	1129
STATUSD DAEMON FOR OBTAINING STATUS INFO FROM NTP (V5.3.0 AND ABOVE)	1129
NTP STATUS SUMMARY TABLE (IN THE NTP SETUP PAGE)	1132
SPECTRACOM REFERENCE CLOCK DRIVER (127.127.45.0)- "TSYNC(0)"	1133
NTP ORPHAN MODE/ORPHANWAIT / UNDISCIPLINED LOCAL CLOCK REFERENCE (127.127.1.0)	1136
*RFC 2783 (PPS CLOCK DRIVER, 127.127.22.0)	1139
SIGNAL 15 ("NTP EXITING ON SIGNAL 15") OR OTHER SIGNALS	1139
WEB BROWSER NTP CONFIGURATIONS	1139
NTP DRIFT FILE	1139
NTP.CONF FILE	1140
DEFAULT NTP.CONF FILE SETTINGS AND THEIR PURPOSES	1140
INHIBIT EPHEMERAL PEERS (RESTRICT NOPEER)	1141
KISS OF DEATH PACKETS (KOD) FOR SECURESYNC/9400S	1142
NTP VERIFICATION/NTP TROUBLESHOOTING	1142
**CLOCK STATUS / NTP PRECISION VALUE	1142
USING THE NTPQ -P OR NTPQ -PN COMMANDS (PEERS COMMANDS)	1143
USING THE "NTPDATE" COMMAND	1146
VERIFYING IF NTP IS ACTUALLY RUNNING	1147
**LOGS FOR NTP	1148
NTP SETUP PAGE DOESN'T SHOW ANY FIELDS (LIKE A BLACK PAGE)	1148
**HOME PAGE INTERMITTENTLY NOT SHOWING NTP STRATUM	1148
*DEDICATED NTP INPUT- PERIODIC HOLDOVER ALARMS BEING ASSERTED	1148

**NTP PEERING (NTP PEERS AND NTP SERVERS)	1149
****THE NEWER BROWSER DOESN'T PROVIDE THE ABILITY TO EDIT/DELETE ANY NTP PEERS OR SERVERS	1149
****NTP PEERING OF SECURESYNCS IN SIMULCAST APPLICATIONS	1149
****NTP PEERS AND NTP SERVERS STATUS/LIMITED REACH/UNREACHABLE SERVER	1151
TOS COMMAND	1152
MINSANE AND MINLOCK: ABILITY TO INCREASE THE NUMBER OF PEERS THAT CAN TURN GREEN (ALL OTHERS BEING "FALSETICKERS")	1152
**KHTD (KTS HOST TIME DAEMON FOR STRATUM 2 OPERATION)	1157
****DEDICATED NTP INPUT- PERIODIC HOLDOVER ALARMS BEING ASSERTED	1157
NTPMOND: STATISTICS LOGGING (CLIENT AND SERVER NTP PACKETS PER SECOND- "PKT/S")	1158
NTP LOADING-NTP THROUGHPUT/NTP STATISTICS: NUMBER OF NTP REQUESTS PER SECOND/NTP STRESS TEST	1159
NTP LOADING/NTP LOAD TESTING/NTP THROUGHPUT (BY SOFTWARE VERSION)	1160
NTP STRESS TEST TOOL (CREATED BY SPECTRACOM ENGINEERING)	1163
MANUALLY STOPPING AND RESTARTING NTP	1164
NTPMOND (AUTOMATICALLY RESTARTS NTP)	1164
NTP STEP THRESHOLD (NTP ALSO HAS ITS OWN REFERENCE TIME CHANGE LIMITS, AS WELL)	1166
"VIEW NTP CLIENTS" (NTP "MONLIST", "MRU LIST", NTP CLIENT LIST)	1167
**DESIRE TO VIEW THE "NTP CLIENT LIST" INFO USING CLI INTERFACE	1173
**DESIRE TO OUTPUT THE "NTP CLIENT LIST" INFO USING THE REST API INTERFACE	1174
**DESIRE TO OUTPUT NTP IN LOCAL TIME (INSTEAD OF NTP)	1174
DESIRE TO PREVENT NTP FROM RESPONDING TO EARLIER VERSIONS NTP REQUESTS (NTPV1, NTPV2 AND NTPV3. RESPONDING TO NTPV4 REQUESTS ONLY)	1175
NTP IPv4/IPv6 ACCESS RESTRICTION / NTPQ AND NTPDC (MODE 7)	1176
NTPQ (MODE 6) AND NTPDC (MODE 7)	1180
NTP PEERS COMMAND (NTPQ -P OR NTPQ -PN)	1183
"TALLY CODE":	1183
NTP REFID / REFERENCE ID (.GPS, .PPS, .INIT, .DROP, .STEP, ETC)	1185
NTPQ ASSOCIATIONS (AS)	1190
NTP STATUS/STATISTICS GRAPHS (NTP THROUGHPUT GRAPHS, NTP PERFORMANCE GRAPHS, TIME OFFSET GRAPH)	1195
PKI (PUBLIC KEY INFRASTRUCTURE/PUBLIC KEY CRYPTOGRAPHY) FOR NTP SECURITY	1202
**NTP SYMMETRIC KEY AUTHENTICATION (MD5/SHA1)/NTP.KEYS FILE	1203
**NTP AUTOKEY	1215
**NEED TO RESTART NTP AFTER CHANGING THE GIGABIT CARD CONFIGS	1216
**TIME IT TAKES FOR NTP TO SYNC AFTER POWER-UP:	1216
**NTP LOG ENTRIES	1216
**AUTOMATIC FTP OF NTP STATISTICS	1219
**NTP UNICAST / MANYCAST / BROADCAST/ MULTICAST / NTP OVER ANYCAST	1220
NTP OVER ANYCAST MODE (AKA "HIGH AVAILABILITY" OR "HA")	1226
ETHERNET BONDING (TWO IP ADDRESSES ASSIGNED TO SAME PORT) / LINK AGGREGATION (LACP)	1228
**EBGP (BORDER GATEWAY) PROTOCOL AND OSPF NSSA FEATURE ("OSPF NOT-SO-STUBBY AREA (NSSA)")	1229
TROUBLESHOOTING NTP OVER ANYCAST NOT WORKING (CLIENTS CAN'T SYNC TO THE ANYCAST ADDRESS)	1246
NTP EXPERT MODE	1248
OPERATION AS A STRATUM 2 SERVER (AS OF 10/20/09)	1250
EXTERNAL 1PPS INPUT TO SECURESYNC	1250
HAVE A DEDICATED "STRATUM 2" SECURESYNC REPORT ITS ACTUALLY "STRATUM 1" INSTEAD	1250
NTP CLOCKSTATS, LOOPSTATS AND PEERSTATS	1251
*NTP BURST/IBURST MODE	1251
ISSUES RELATED TO NTP	1251
NOTIFICATIONS / EMAIL ALERTS /SNMP	1253
*NOTIFICATIONS (SNMP TRAPS AND EMAIL ALERTS)/ALARMS	1253
OPT-IDM: AVAILABLE BROADSHIELD NOTIFICATIONS (V5.7.1 AND ABOVE ONLY, AND ONLY WITH OPT-IDM ENABLED)	1256
**NULLMAILER/EMAIL ALERTS	1259
**SNMP (SNMPv1/SNMPv2C/SNMPv3)	1264
**REMOTE MONITORING / SNMP CONFIGURATION	1265
***SysOBJECTID, SysCONTACT AND SysLOCATION FIELDS	1276
SYSNAME FIELD (UNIT'S HOSTNAME IN SNMP)	1276
CPU USAGE (CPU USED) / PROCESSOR USAGE/CPU USAGE 100%	1278
**USING LINUX TO PERFORM SNMPWALKS SNMPGETS SNMPTRAPS	1281
USING SNMPGET COMMAND VERSUS USING EITHERSNMWALK/SNMPGETNEXT COMMANDS (FOR RETRIEVING VALUES FROM AN SNMP TABLES)	1281

<i>SNMPv3 ENCRYPTION INFO/DETAILS</i>	1287
<i>SNMPv3 ENGINE ID FIELD</i>	1290
<i>**TESTING/VERIFYING SNMP/EMAIL ALERTS ARE ENABLED AND WORKING INSIDE THE SECURESYNC</i>	1295
<i>**TROUBLESHOOTING / KNOWN ISSUES WITH SNMP</i>	1297
<i>EXAMPLES OF AVAILABLE SNMP GETS/SETS</i>	1307
<i>PTP MIB FILE (FOR 1204-12 10/100 CARD) AND GB PTP MIB FILE (FOR 1204-32 CARD)</i>	1307
<i>NOTIFICATIONS/TRAPS FOR SAASM RECEIVER ONLY</i>	1314
<i>TESTING SNMP TRAPS AND EMAIL ALERTS</i>	1315
MODELS 9483 AND 9489	1324
<i>LAST TIME BUY (LTB) / END OF LIFE (EOL) / DISCONTINUANCE OF NETCLOCK 9483/9489</i>	1324
<i>VISIO STENCILS/SHAPES FOR THE MODELS 9483 AND 9489</i>	1325
<i>MODEL 9489s</i>	1327
<i>(9489 VERSUS SECURESYNC/9483)</i>	1327
<i>9489 WITH RS-485 INPUT (REPLACEMENT TO THE MODEL 9388s)</i>	1327
<i>MODEL 9483s</i>	1328
<i>(9483 VERSUS SECURESYNC)</i>	1328
<i>POWER CONSUMPTION/HEAT DISSIPATION/GROUNDING AND POWER SUPPLIES</i>	1328
<i>PS06R-2Z1M-DT01 (AVAILABLE AC TO DC CONVERTER FOR REDUNDANT AC INPUT)</i>	1328
<i>MSF/WWVB/DCF77</i>	1329
SPECIFIC OPTIONS FOR 9483s ONLY	1329
<i>OPTIONS SUMMARY FOR 9483 ONLY</i>	1329
<i>OPTION 12: PTP INPUT/OUTPUT (MODEL 1204-12 PTP CARD)</i>	1329
<i>OPTION 13: T1/E1 OUTPUTS (MODEL 1204-0A OPTION CARD)</i>	1329
<i>OPTION 14: ADDS 12VDC INPUT FOR REDUNDANCY</i>	1329
<i>OPTION 15: ADDS 24VDC INPUT FOR REDUNDANCY/ DESIRE TO USE PS06R-2Z1M-DT01</i>	1330
<i>OPTION 16: MULTI-PORT GIGABIT OPTION CARD (ADDS THREE 10/100/1000 BASET) (MODEL 1204-06)</i>	1330
<i>OPTION 17: PROGRAMMABLE TTL OUTPUT CARD (MODEL 1204-??)</i>	1330
<i>PASSWORD RESET WHEN CURRENT SPADMIN PASSWORD IS NOT KNOWN MODEL 9489 ONLY)</i>	1331
<i>NETWORK PORTS / CONFIGURATION (IP ADDRESS, GATEWAY ADDRESS,</i>	1331
<i>NETMASK SETTINGS</i>	1332
<i>ASCII RS-485 ("ASCII OUTPUT 1") OUTPUT CONFIGURATION</i>	1334
<i>SOFTWARE VERSIONS/UPDATES/ISSUES</i>	1336
<i>SYSTEM LOGS</i>	1336
<i>SNMP (MIBS/TRAPS/OID NUMBERS/EMAIL ALERTS)</i>	1337
<i>LOCAL SYSTEM CLOCKS (LOCAL CLOCK)</i>	1337

General Safety

- Refer to Salesforce Cases such as: [282804](#)

Suggestions:

- Refer to “**Safety**” (such as Electrical safety) in the online SecureSync user guide https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/INSTALL/Safety.htm
- Refer to **RB oscillator MSDS datasheet and disposal** docs: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Oscillators, rb material\Rb oscillator>
- Refer to **lithium battery replacement** in all SecureSyncs (note there is also a lithium battery for SAASM receiver, if installed): <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement>
- Refer to the “**Regulatory Compliance**” section of the online user manual for info on FCC, Safety (UL 60950), CSA, EMI/MC and CE: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INTRO/Compliance.htm
- Refer also to the “**UL and CE Testing / Declarations of Conformity**” section of the custserviceassistance doc for additional info: <..\CustomerServiceAssistance.pdf>

Email from Tom Richardson 7/16/12 KW: SecureSync is CE, UL and FCC certified.

- Refer to the “**Regulatory Compliance**” section of the online SecureSync (or NetClock) user guide for info on FCC, Safety (UL 60950), CSA, EMI/MC and CE: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INTRO/Compliance.htm

FCC

This equipment has been tested and found to comply with the limits for a **Class A digital device**, pursuant to **Part 15 of the FCC Rules**.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a **commercial environment**. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the user documentation, may cause harmful interference to radio communications.

Operation of this equipment in a **residential area** is likely to **cause harmful interference** in which case the user will be required to correct the interference at his/her own expense.



Note: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Safety

This product has been tested and meets the requirements specified in:

- EN 60950-1:2006/A11:2009 +A1: 2010 +A12: 2011 +A2:2014, UL 62368:2014
- UL 60950-1:2007 R10.14 CAN/CSA C22.2 No. 62368-1-14
- CAN/CSA-C22.2 No.60950-1-07+A1:2011+A2:2014
- IEC 62368-1:2014
- IEC 60950-1:2006 +A1+A2 EN62368-1:2014
- UL Listing no. E311040

EMC Compliance

This product has been tested and meets the following standards:

- EN 55032:2012/AC:2013/CISPR 32:2012: Class A
- CAN/CSA-CISPR 22-10/ ICES-003 Issue 6: Class A
- FCC CFR 47 PART 15 SubPart B:2016: Class A
- EN55024:2010: Class A

European Directives

This product has been tested and complies with the following:

- 2014/30/EU Electromagnetic Compatibility (EMC)
- 2014/35 EU Low Voltage (LVD)
- 2011/65/EU on the Restriction of Hazardous Substance (RoHS3)
- 2014/53/EU Radio Equipment Directive (RED)
- Radio Spectrum Efficiency:EN 303 413 V1.1.0

- Refer also to the “**UL and CE Testing / Declarations of Conformity**” section of the custserviceassistance doc for additional info: [..\CustomerServiceAssistance.pdf](#)
- Main Link to CB testing/EMC-ESD testing / CE and Declaration of Conformity (DoC) and associated documents for SecureSyncs and 9400s: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CE Declaration of Conformity and EMI-EMC](#)

SAFETY: Regulatory Compliance: UL / FCC/ EMC-ESD / EMI / CB testing / Rohs-CE / Compliance / Declaration of Conformity (DoC)/IEC-60950-1/IEC-62368/EN 55032

CE Declaration of Conformity (DoC) for SecureSync/9400s

- DoC (in Arena, attached to the [DEC-CONF-SECURESYNC](https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508&orb_msg_single_search_p=1) item): https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508&orb_msg_single_search_p=1

from Tom Richardson (15 May 18) BTW and for your information. The test reports for the SecureSync are available in Arena PLM attached to the DEC-CONF-SECURESYNC item. That is also where the latest declaration of conformity can be found.

A) SecureSync CE approval/Declaration of Conformity

- The SecureSync is CE compliant, so a Declaration of Conformity is available upon request.
- The “Declaration of Conformity” document (DEC-CONF-SecureSync”) is stored in Arena at: https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508
 - **Per Dave Sohn (15 Jun 15):** it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

B) 9483/9489 CE approval/Declaration of Conformity *(including EMI/EMC testing)

- The 9400 series is CE compliant, so a Declaration of Conformity is available upon request.
 - The **SecureSync** CE Declaration of Conformity document is stored in Arena (refer to link above)

Leakage current (current leakage)

- Refer to Salesforce case 163902
- Refer to reports (in Arena): https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508&orb_msg_single_search_p=1

Leakage current is the **current** that flows from either AC or DC circuit in an equipment to the chassis, or to the ground, and can be either from the input or the output. If the equipment is not properly grounded, the **current** flows through other paths such as the human body.

LTA (Danny: Land Transport Authority) is looking for the a test report of current leakage of all equipment
The link below is an explanation of what they want to see.

<http://carelabz.com/what-leakage-current-testing-measuring-how-leakage-current-testing-measuring-done/>

Emai from Tom Richardson to Danny Loke (15 May 18) I think figured out what you were looking for. Please reference the attached CB report, section 5.1 on Touch Current and in particular 5.1.6 and table 5.1. This states the measured touch current for the SecureSync product line. We are a Class 1 device and the current is required to be less than 3.5 mA. Also, we put the UL mark on the SecureSync and the product is 100% tested in the factory for Hi-Pot and Ground Bond.

Follow-up from Tom Richardson (15 May 18) BTW and for your information. The test reports for the SecureSync are available in Arena PLM attached to the DEC-CONF-SECURESYNC item. That is also where the latest declaration of conformity can be found.

Flammability testing/certification

- Refer to the SecureSync IEC 60950-1 IT Equipment report (“31683550.001 CB Complete.pdf”) : <I:\Customer>

[Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\EMC and CE Declaration of Conformity\CE testing](#)

- Refer to reports (in Arena): https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508&orb_msg_single_search_p=1

Fire retardent chemicals (bromine/inorganic phosphorus material)

Q from a customer: Is there any about inorganic phosphorus material in SecureSyncs?

A Per Tom Richardson (6 Dec 17) "We have determined, according to our documentation, that there is no inorganic phosphorus material in the SecureSync. Bromine is the chemical used as the fire retardant in our boards."

Earlier Email from Tom Richardson to Josh (5 Dec 17) I have finally received a reply back from our PCB assembler. They use many different board materials for our circuit boards. They can narrow it down faster if you know why the question has come up? Also is there a specific type of phosphorus they are looking for? There are organic and inorganic phosphates, phosphonates, phosphinates as well as red phosphorus that can be used as flame retardant in PCBs.

EMI-Emissions/EMC/ESD testing

Email from Josh to TOYO (Oct 2017): As an update, we had the SecureSync re-tested in 2016/2017 for emissions and safety.

ESD IEC-61000-4-2 level (1,2,3,4,x) - Level 3, 8kV air discharge

STD IEC 62236-4 / desire to perform surge testing of the RF input to the GNSS receiver

- Search for "STD IEC 62236-4" in the Customerserviceassistance doc (link to this document further above)
- Refer also to Salesforce case 24513

Fundamental frequency for SecureSyncs

Q A while back I asked you if the SecureSync was tested to FCC Class B EMI emissions and you told me it wasn't, only to FCC Class A. We are testing it to class B this week and we have a question. **Do you know the fundamental frequency of the unit?** Typically that is the processor speed. Knowing that value helps us determine which frequencies to test the unit to. Any input would help.

A Response from Dave Sohn (6 Oct 16) We tested based on a maximum usable frequency of **500MHz** of the processor.

UL Testing/ UL certificates

- Refer to reports (in Arena, attached to the DEC-CONF-SECURESYNC item): https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508&orb_msg_single_search_p=1
- Refer to UL Test report in Sharepoint: https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/_layouts/15/osssearchresults.aspx?u=https%3A%2F%2Foroliagroup-portal1.sharepoint.com%2FSpectracom%2FEngineering%2Fproducts%2FSecureSync&k=conformity

UL94HB level (V2,V1,V0,5VB,5VA) - The circuit board is 94V0

***Touch current

- Refer to Salesforce case 163902

Note the CB report referred to in email below ("31383550.001 CB complete.pdf") is in: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CE Declaration of Conformity and EMI-EMC](#)

Email from Tom Richardson to Danny Loke (15 May 18) I think figured out what you were looking for. Please reference the attached CB report, section 5.1 on Touch Current and in particular 5.1.6 and table 5.1. This states the measured touch current for the SecureSync product line. We are a Class 1 device and the current is required to be less than 3.5 mA. Also, we put the UL mark on the SecureSync and the product is 100% tested in the factory for Hi-Pot and Ground Bond.

Tests/SecureSync Test Reports

C) IEC 60950 / EN 60950 / UL 60950 (Product Safety testing standard for “Information Technology Equipment”)

- Refer to Salesforce Case 256342 (Jan 2021)
- Test report at: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CE Declaration of Conformity and EMI-EMC\IEC 60950 test report>

D) IEC 55032 / EN 55032 (Electromagnetic compatibility of multimedia equipment. Emission Requirements)

- Refer to Salesforce Case 256342 (Jan 2021)
- Refer to sites such as: <https://www.dlsemc.com/iec-en-55032-electromagnetic-compatibility-of-multimedia-equipment-emission-requirements/>

RoHS compliancy statement for SecureSyncs and 9400s

General info on RoHS / RoHS2 / RoHS3 Compliancy:

Refer to:

- <https://www.rohsguide.com/>
- “RoHS in: <..\CustomerServiceAssistance.pdf>

RoHS 2 versus RoHS 3

- Refer to s here : <https://www.rohsguide.com/rohs3.htm>

[RoHS 2 vs RoHS 3 \(EU 2015/863\)](#)

Guide to RoHS 3 Compliance: Regulations, Exemptions, Certification, Initiatives. RoHS 3 (EU 2015/863) RoHS 3 (EU Directive 2015/863) adds Category 11 (catch-all) products and adds four new restricted substances - all phthalates.

www.rohsguide.com

RoHS compliancy for Model 1200 SecureSyncs/9400s (and associated AC power cord CA06R-1513-0001)

- Refer to the SecureSync data sheet and Declaration of Conformity
 - For a link to the current Dec of Conformity, go to: [CE Declaration of Conformity for SecureSync/9400s](#)
 - Refer to reports (in Arena): https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508&orb_msg_single_search_p=1

Your question

Q Could you please inform us if the items listed below are RoHS compliant?

GPS Clock Serial Card P/N 1204-02

GPS Clock P/N 1200-0273-0601

A reply from Keith (15 Mar 17)

My response

The Spectracom SecureSync (Model 1200 series), as well as all of the SecureSync's available Option Cards (Model 1204 series) are RoHS compliant.

Attached for your reference is a copy of the SecureSync data sheet. Excerpted below from page 3 of this document are the Agency Approvals for these two items:

Agency Approvals

CE, UL, cUL, CSA, FCC part 15 class A, ROHS, WEEE

Note that I have also attached a copy of the CE Declaration of Conformity, as well- just in case you may require it ☺!

MIL-STD-461 (ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS)

- Refer to sites such as: <https://en.wikipedia.org/wiki/MIL-STD-461>
- Refer to Salesforce Cases such as 196350

MIL-STD-461^[1] is a [United States Military Standard](#) that describes how to test equipment for [electromagnetic compatibility](#).

Various revisions of MIL-STD-461 have been released. Many military contracts require compliance to MIL-STD-461E. The latest revision (as of 2015) is known as "MIL-STD-461G".^[2] While MIL-STD-461 compliance is technically not required outside the US military, many civilian organizations also use this document.^[3]

Electromagnetic compatibility test labs typically set up their [anechoic chamber](#) to comply with MIL-STD-461. Test labs attempt to comply with this standard for two reasons

Q It is not mentioned in the Datasheet that SecureSync is compliant with MIL-STD-461. However, in every EMC Test reports available in Arena, it mentioned by Chomerics Test Services that:

Chomerics test facility operates under the current revision of Chomerics Quality Assurance (QA) Manual Document Number QA002.

The QA Manual has been constructed to reflect a quality program in accordance with the requirements of the National Institute of Standards and Technology (NIST), ISO 9002, ISO 17025, ISO Guide 25, NIST Handbook 150, EN 45001, MIL-I-45208A, MIL-STD-461D, 462D and Chomerics Quality Assurance Program (QAP).

The QA Manual outlines and describes the procedures for establishing and maintaining the quality of analysis, research, inspection, and testing within Chomerics Test Service (CTS).

This test report does not represent an endorsement by the U.S. Government.

The results and/or conclusions within this test report refer and/or apply only to the unit(s) tested as defined by this report.

Measurements performed for this test are traceable to the National Institute of Standards and Technology (NIST) based on the fact that all test equipment used for the measurements were previously calibrated using standards traceable to NIST.

Q We need confirmation that 1204-1C, 1204-11, 1204-06, 1204-32 and 1200-033 comply with MIL-STD-461.

A reply from Dave Sohn (27 May 2019) SecureSync is not compliant with MIL-STD-461. The test house, Chomerics, is capable of testing to that standard, which is why they list that in their documentation.

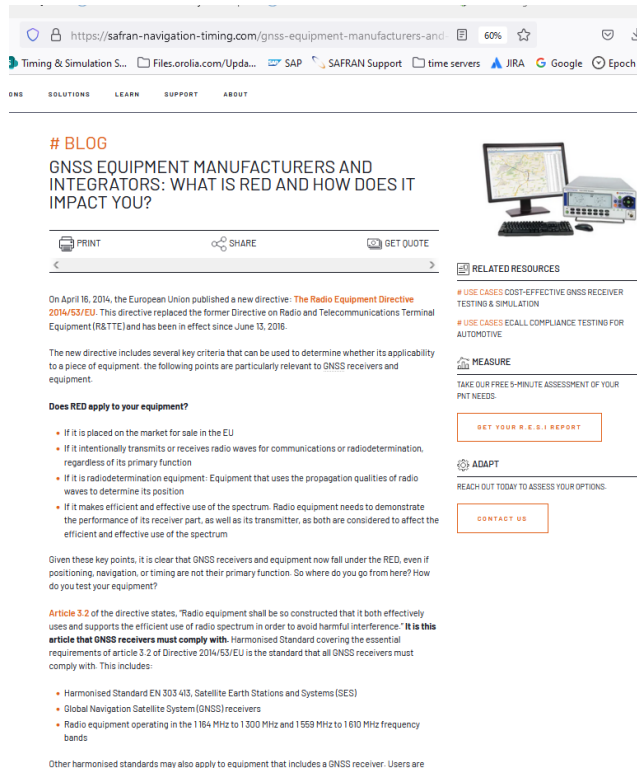
Consider VersaSyncs (instead of SecureSync) if MIL-ST-461 is a requirement

Partial Email from Sylvain to Tony Diflorio (11 June 2020) Securesync has not been designed and tested for MIL-STD-461.

You can refer to VERSASYNC for such case : http://manuals.spectracom.com/VSS/Content/VSS/INTRO/VSS_Compliance.htm
So if MIL-STD-461 is mandatory for them, we should find a corresping configuration based on VersaSync plateform (if the form factor is acceptable for them).

Article 3.2 of the EU Radio Equipment Directive (RED) / ETSI EN 303 417: Wireless power transmission systems (WPT)

- Refer to Salesforce Case 300857
- Refer to sites such as
 - Blog on our website: <https://safran-navigation-timing.com/gnss-equipment-manufacturers-and-integrators-what-is-red-and-how-does-it-impact-you/> (excerpt below)



- https://www.etsi.org/deliver/etsi_en/303400_303499/303417/01.01.01_30/en_303417v010101v.pdf (excerpts below)

1 Scope

The present document specifies technical characteristics and methods of measurements for wireless power transmission (WPT) systems, using technologies other than radio frequency beam, in the 19 - 21 kHz, 59 - 61 kHz, 79 - 90 kHz, 100 - 300 kHz, 6 765 - 6 795 kHz ranges.

The present document covers wireless power transmission systems which are regarded as radio equipment since including inherent radio communication functionality or radiodetermination via the WPT interface or port at the specific WPT frequency ranges.

Such systems usually consist of:

- 1) A power transmitter, with additional communication capability to control the charge function, in conjunction with the receiving part. The power transmitter could also be named as base station.
- 2) A power receiver, which supplies the received energy to a mobile device and performs a control/supervision function for the mobile device status and charge operation. Both parts in combination are able to transmit and receive data in addition to the power transmission mode e.g. to control the mobile device status and to optimize the power transmission mode.

These radio equipment types are capable of operating in the permitted frequency bands below 30 MHz as specified in Table 1.

The present document covers fixed systems, mobile and portable systems.

Table 1: WPT systems within the permitted frequency bands below 30 MHz

WPT frequency range	Frequency Bands	Applications
Transmit and Receive 1	19 kHz to 21 kHz	WPT systems
Transmit and Receive 2	59 kHz to 61 kHz	WPT systems
Transmit and Receive 3	79 kHz to 90 kHz	WPT systems
Transmit and Receive 4		

4

100 kHz to 119 kHz WPT systems

Transmit and Receive 119 kHz to 140 kHz WPT systems

Transmit and Receive 140 kHz to 148,5 kHz WPT systems
Transmit and Receive 148,5 kHz to 300 kHz WPT systems
Transmit and Receive 5 6 765 kHz to 6 795 kHz WPT systems

NOTE 1: The frequency ranges listed in Table 1 are also used for generic inductive short range devices, according to ETSI EN 300 330 [1].

NOTE 2: The limits and the frequency ranges of the present document are EU wide harmonised according to EC Decision 2013/752/EU [i.2] and ERC/REC 70-03 [i.1].

NOTE 3: In addition, it should be noted that other frequency bands may be available in a country within the frequency range below 30 MHz

4.2.1 Background information

In this clause all general considerations for the testing of wireless power transmission (WPT) systems using technologies other than radio frequency beam in the 19 - 21 kHz, 59 - 61 kHz, 79 - 90 kHz, 100 - 300 kHz, 6 765 - 6 795 kHz ranges are given. The tests cover all different operational modes, as described in clause 4.2.3.

4.2.2 Wanted performance criteria

A WPT system always consists of a base station and a mobile device which are in proximity to each other. The performance of a WPT system is dependent on the related operational mode, see clause 4.2.3.

For the purpose of the receiver performance tests, the WPT system shall produce an appropriate output under normal conditions as indicated below:

- use as intended without degradation of performance; or
- a degradation of the performance is indicated by the WPT system as described in the manual.

The manufacturer shall declare the performance criteria used to determine the performance of the receiving parts inside the WPT system (related to the mode)

DISA/STIGS (Security Technical Implementation Guides)/SRGs (Security Requirements Guides) for all products

- Refer to sites such as: <https://public.cyber.mil/training/srgs-and-stigs-training/>
- Refer to Salesforce Cases such as 231198 (April 2020), 187142 (Feb 2019) and 24204 (Jan 2017)

Note: the best source of info about securing/hardening the SecureSync for security is the “**Default and Recommended Configurations**” section of the online 1200 SecureSync user guide:

https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/ADMIN/Conf_Def_Recom.htm

STIGs (Security Technical Implementation Guide) are the guidelines that **DISA** publishes for certain components of information technology and communication infrastructure used by the defense community that **DISA** supports. ... **SRG** is short for **Security Requirements Guide**.

From: https://en.wikipedia.org/wiki/Security_Technical_Implementation_Guide

A **Security Technical Implementation Guide (STIG)** is a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. These guides, when implemented, enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities.

Examples where STIGs would be of benefit is in the configuration of a [desktop computer](#) or an enterprise server. Most operating systems are not inherently secure,^[1] which leaves them open to criminals such as identity thieves and computer hackers. A STIG describes how to minimize network-based attacks and prevent system access when the attacker is interfacing with the system, either physically at the machine or over a network. STIGs also describe maintenance processes such as software updates and vulnerability patching.

Advanced STIGs might cover the design of a corporate network, covering configurations of routers, firewalls, domain name servers and switches.

General Email from Dave Sohn (27 Apr 2020, relating to Salesforce Case 231198) “We have not evaluated the SecureSync against any STIGs, in order to provide the feedback he is looking for. We can help on specific questions that they may have.”

Keith’s response to customer

To begin, we have not evaluated the SecureSync against any STIGs, in order to provide the feedback you are looking for. However, we can help you with any specific questions that you may have, pertaining to the operation of the SecureSync.

For example, a customer once stated they needed to have support of a login banner when connecting to SecureSync, due to STIGs. We responded that the SecureSync does support login banners for both the web browser and CLI interfaces. And we provided the link to the particular section of the online SecureSync user guide which discusses info on creating login banners.

Note the online SecureSync user guide is a great reference. It contains the most up to date info about the operation of SecureSync, and is very easily searched by ‘key words’. Here is the link to the home page of this great reference: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INTRO/Getting_Started.htm.

In general, I can also let you know that for file integrity purposes, we do not provide elevated/su login to the SecureSync, nor release its root password/root level access to anyone outside of the Orolia Engineering team.

Please don’t hesitate to let me know if you have any specific questions associated with STIGS/SRGs, as they may pertain to the operation of SecureSyncs.

Email from Bill Glase (3/5/12) Leisa, if it helps you can send them a copy of our CIP-7 Security Report (on our internal network [here](#)) as an example of the security assessments we do. It is not a STIG compliance statement though.

<https://oroliagroup-portal1.sharepoint.com>

<https://oroliagroup->

portal1.sharepoint.com/ppsecure/post.srf?wa=wsignin1%2E0&rpsnv=2&ct=1333973817&rver=6%2E1%2E6206%2E0&wp=MBI&wreply=https%3A%2F%2Fwww1877%2Esharepoint%2Ecom%2F%5Flayouts%2Fanding%2Easpx%3FSource%3Dhttps%253A%252F%252Fforliagroupemicrosoftonlinecom%252D1%252Esharepoint%252Eemea%252Emicrosoftonline%252Ecom%252F%255Fforms%252Fdefault%252Easpx&lc=1033&id=500046&cbcxt=mai&wldp=1&guest=1&bk=1333973817

Email from Paul Myers (3/5/12)

NOTE: We support NTP which is good.

NTP security has NOT been an issue so far, but I doubt we meet any STIG if it describes security.

Our NTP Supports security which includes Symmetric Keys and a single configuration of the AUTOKEY 'IFF protocol'.

Our AUTOKEY implementation is the most basic and supports IFF Group and Client Keys. We only support RSA keys and MD5 hash.

This is NOT likely the preferred method and we don't use a FIPS OpenSSL if that is require

Email from Paul Myers (3/5/12)

I don't believe we support the Military Key Distribution schemes. Otherwise Mark Goodlein would have pointed this out in his research of the STIGS.

I can report what we currently support. NOT compliance to specific STIGs as Mark Goodlein did this research.

➤ **In regards to SSH:**

- We do not support any "Certificates" for SSH.
- SSH uses Public Keys.
- We allow the user to Load Public keys via the Web UI.
- The current public keys can be added to by adding text at the end of the list or by replacing entirely what is there.
- The user can create a single or list of public keys into the web browser.
- The number of public keys typically corresponds to 1 key per user. I was able to load a several key file.
- Public key length depends on the number of bits in the key and key type. A key file is typically 1-2Kbytes in my experience, but STIG compliant keys could be longer????
- Our code does not limit the length of the key file. SSH does not limit the number of public keys that I am aware of.
- A bug seems to exist in the Web UI which can cause the Web UI to fail to return after loading a LARGE key file of several kilobytes. The key file is loaded, but the connection is lost. I tried to load a 10Kbyte keyfile and the file was loaded, but I had to reconnect to the web ui. This will be investigated.

➤ **In regards to HTTPS:**

- Certificates are used for HTTPS sessions. We only support the following.
- Loading x509 PEM certificates from the Web UI – Default for APACHE web server
- We support the user loading Public Keys via FTP by specific filename and then selecting then enabling that certificate for use using the WebUI
- This could be improved on with a better web UI but so far no one has complained or even used it I believe.
- We convert the following certificates from these types identified by file name to the x509 PEM used by Apache
- FTP a file named cert.pem which means x509 PEM
- FTP a file named cert.der which means x509 DER
- FTP a file named certpem.p7c which means PKCS7 PEM

- FTP a file named certder.p7c which means PKCS7 DER

NTP authentication (not using MD5)

- Refer to Salesforce Case 024204

Q The latest guidance **deprecates MD5 encryption**. NET0813 STIG states: "Review the network element configuration and verify that it is authenticating NTP messages received from the NTP server or peer using either PKI or a FIPS-approved message authentication code algorithm. FIPS-approved algorithms for authentication are the cipher-based message authentication code (CMAC) and the keyed-hash message authentication code (HMAC). AES and 3DES are NIST-approved CMAC algorithms. The following are NIST-approved HMAC algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256." Fix: "Configure the device to authenticate all received NTP messages using either PKI (supported in NTP v4) or a FIPS-approved message authentication code algorithm"

Can you confirm for us whether other non-MD5 encryption authentication methods are available for the 12xx line? AES/3DES/SHA-x or PKI are acceptable solutions but I could not find documentation about how to implement alternatives, if this is possible. Thanks.

A reply from Keith (20 Jan 2017) My response The Spectracom SecureSync provides the ability to either select either MD5, or a different Digest scheme (such as SHA, SHA1 or a couple of others) for NTP Authentication. The below screenshot shows the available schemes (in addition to MD5) that can be configured in the Management -> NTP Setup page of the SecureSync's web browser (click on the "Symmetric Keys" button on the left side of the page. Then press the "+" sign in the upper-right corner of the pop-up window that opens):

Add SSH timeout to allow NISSUS Scan to pass

- Refer to Salesforce Case 187142 (Feb 2019)

Q I have one comment that I believe you guys need to put in the next release, as with the Web Interface Settings configuration to you have a logout timeout in minutes for Idle. You need to add that for SSH sessions too, to pass DISA STIG I have to disable the SSH facility. This need to be added asap, you should get the Nessus scanner and test credentialed scan for all release for DOD deliverables.

A reply from Dave Loto Dave Sohn:Hi Dave, Here is a suggestion from our friend Ed Mayers at USAF. He advised we should implement a SSH timeout setting like we have for the web UI

Need for login banner

- Refer to Salesforce Case 217824

Q "We have several SecureSync systems, and are implementing DISA STIGs. One of the STIGs requires a MOTD banner that states "You are logging into a government information system, etc, etc...". In order to add this banner, we need write access to /etc/motd which is owned by the root user."

A Keith's response (Dec 2019) To begin, and for file integrity purposes, we do not release the SecureSync's root level password to anyone outside of the Orolia Engineering team. However, the good news is the desired login banner can be created using standard admin rights (such as via the spadmin account).

The CLI and Web browser banners are not stored in, and don't require access to etc/motd (which just stores the current software version). These login banners can be created in the unit's web browser. For more information on creating a login banner for CLI and/or the web browser, please see the "Creating a Login Banner" section of the online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/Banner.htm.

Customer report: DISA STIG requirement that the spadmin account password never expires

- Refer to SF case 117138

Q The password expiration for the user "spadmin" when we turn on the password policy and are required to change the default shipping password is a CAT 1 DISA STIG failure that will block deployment into the network. We are using the "spadmin" account as the emergency access account per DISA STIG requirements and the new password should not expire to be compliant. Is there a way to disable this for this account or can we create a true non-expiring emergency account?

A Reply from Dave L (~23 Aug 17) I believe all accounts are governed by the same rules and we cannot separate the spadmin from User accounts but I will check and verify this. Please standby while I confirm.

Created By: [Ron Dries \(10/17/2017 2:47 PM\)](#) | Last Modified By: [Ron Dries \(10/17/2017 2:47 PM\)](#)

The directory '/var/db/pkg' did not exist in either software versions 5.4.1, or 5.6.0. I am not sure how the Nessus credentialed scan would have passed at 5.6.0 as it should not have been able to find '/var/db/pkg'. There is the potential that the Nessus scan updated, or changed. Further investigations needs to be performed to see if a change in SecureSync software could be causing the issue.

Dave Sohn (24 Aug 17) The spadmin account password can be reset to default at any time via the front panel, if necessary. Is that acceptable to resolve the issue?

Questions/Answers

➤ from Salesforce Case 231378 (May 2020, with 5.8.8 being the current version)

Reply from Ron Dries (8 May 2020) -answers in red

- Are local users passwords encrypted when stored on the device, and if so, what encryption algorithm is used?
The local users are stored using standard Linux password hashing, using an MD5 hashing algorithm.
- Does the device use FIPS-validated HMAC to protect the integrity of nonlocal maintenance and diagnostic communications?
We support connections via HTTPS secured using TLS. The version of TLS and the ciphers available can be restricted via Web UI configuration.
- Is there any way to limit the number of concurrent sessions to both the web GUI and CLI? And is there a way to configure it to generate audit records when concurrent logons from different workstations occur?
Concurrent sessions to the Web GUI and CLI are not configurable. Only a single user session is allowed to the Web UI. We do not have a logging mechanism for concurrent logins from different workstations.
- Does the device control where management information is allowed to travel within itself, and if so, how?
Each ethernet port has its own routing table that can be configured, this can also be handled on the switch that the SecureSync is connected to.
- Is there any way to configure the device to generate a real-time alert for audit failures?
SecureSync does have SNMP traps and email alerts that are configurable.
SNMP: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Traps.htm
Notifications: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/Notificat_Conf.htm
- Is there any way to configure the password policy to require that when a password is changed, the position of at least 8 characters is changed?
Password policy: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/Passwords.htm
- Is there any way to invalidate sessions identifiers when an administrator logs out? This is referring to webUI sessions?
"When a user logs out of the web UI, the session is invalidated."
- Does the device recognize only system-generated session identifiers, and if so, does it generate them with a FIPS-approved random number generator?
We utilize OpenSSL in SecureSync but I am not sure if it is FIPS approved. Our OpenSSL version is 1.0.2o.

- How often are audit logs pushed to the remote log server, and if it is greater than 7 days, is there any way to configure it as such?

After configuring syslog on a SecureSync it will send logs to the remote log server when they are written on the device.
remote logging: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/Logs_Configuring.htm

Remote log server configuration:

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/Logs_Remote%20Servers.htm

- Does the device conduct backups of system level information, and if so, where is it stored, and can it be exported? And if changes occur, are backups taken?

Configuration backups can be initiated on the SecureSync through the CLI or webUI. The CLI will store the config bundle on the local file system where it can be copied off. The webUI will store the config bundle on the local file system as well as download it to the user's computer.

This process is not scheduled by default and is a manual operation. However there are ways to automate it.

Information Assurance (IA) / Common Criteria (CC) / EAL levels

- Refer to the “Information Assurance (IA) / Common Criteria (CC) / EAL levels” section in the [custserviceassistance](#) document.

Sounds similar to FIPS, but FIPS is a government security standard while IA appears to be an International standard

From Wikipedia:

Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of [information security](#) which in turn grew out of practices and procedures of [computer security](#).

From Wikipedia:

The **Common Criteria for Information Technology Security Evaluation** (abbreviated as **Common Criteria** or **CC**) is an [international standard](#) (ISO/IEC 15408) for [computer security](#) certification. It is currently in version 3.1.^[1] Common Criteria is a framework in which computer system users can *specify* their security *functional* and *assurance* requirements, vendors can then *implement* and/or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims. In other words, **Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.**

Email from Tony Diflorio to a customer (8/3/12) We do not have a formal IA certification, but have evaluated the SecureSync against industry standards such as CIP-7, and HIPAA. We regularly scan the product for security vulnerabilities using a commercial assessment tool.

The CC Eval does not typically apply to a product that is providing "Time" over a network. So the answer is "not evaluated". Please let us know if you need further information.

FIPS compliancy (FIPS 140-2) /CIP/NERC/Cyber Security/Potential Vulnerabilities/Anti-virus software/ CSG security accreditation

E) FIPS Compliancy (FIPS 140-2)

- For info on FIPS, refer also to:
 - FIPS (in [..\CustomerServiceAssistance.pdf](#))
 - FIPS-140 validation: <https://www.openssl.org/docs/fips.html>

Here is some information on the Securesync cybersecurity:
<https://www.rolia.com/knowledge-center/resilient-pnt-cybersecurity>

Sub-topics associated with FIPS compliancy

1. HSTS (HTTP Strict Transport Security)

- Refer to "[HTTP / HSTS \(HTTP Strict Transport Security\)](#)" in this document

2. Network Isolation/Network security/FIPS compliancy

- Refer to (in this document): [** Network Isolation/Network security/ FIPS compliancy](#)

3. OpenSSL

- Refer to FIPS-140 validation: <https://www.openssl.org/docs/fips.html>

FAQs for FIPS compliancy

Q Can the SecureSync 1200 be configured for FIPS compliance?

A I have checked and **Orolia does not claim FIPS 140-2** Compliancy on the Securesync products.

Q. **Email from Jeremy Thomas (10/13/11)** "They site CSG security accreditation (EL4 and above) no doubt we have similar US alternatives"

A. **Reply from Dave Sohn:** We don't have any security accreditations for the SecureSync

Q. **Email from Jeremy Thomas (10/13/11):** The question is the separation and security of SecureSync network timing signals as each test room must ensure absolute security

A. **Reply from Dave Sohn:** Network isolation is handled within the SW via routing tables and rules.

F) CIP (Critical Infrastructure Protection) for NERC (North American Electric Reliability Corporation)

- Refer to <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
- Refer also to: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Security- Vulnerabilities -PCI compliance](#)

NERC compliancy- refer to Salesforce Cases such as 214097

Q. I have a customer who uses the Spectracom SecureSync Time Server with their network setup for a Distributed Control System at a power plant. To be NERC Compliant, they need documentation stating that this product does not support antivirus, or the ability for whitelisting. Is it possible to get an official attestation so I can provide it to my customer?

Description of CIP: A list of various Standards for the Power industry/Power grid

Email from Keith to Gerry Gasca (26 June 2018): To begin, our understanding of CIP-010-2 and COP-007-6 is that we need to describe open "listening" ports and any associated services to those ports (not every service that is running in the SecureSyncs, as you had requested).

Based on the changes you've incorporated to the settings of the SecureSync, below is a list of the remaining **open ports**, and their **associated services**:

G) CIP-007 (CIP-7) ("Cyber Security - System Security Management")

- Refer to http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-007-6&title=Cyber%20Security%20-%20System%20Security%20Management&jurisdiction=null
- Refer to "SecureSync-CIP007-Secury-Compliance-Report.pdf" at the following link: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Security- Vulnerabilities
- Refer to Salesforce cases (such as for Gerry Gasca)

From Dave Sohn to Matt Loomis (13 Mar 2013) We had put together a NERC CIP-007 document for SecureSync some time ago. This might help the customer.

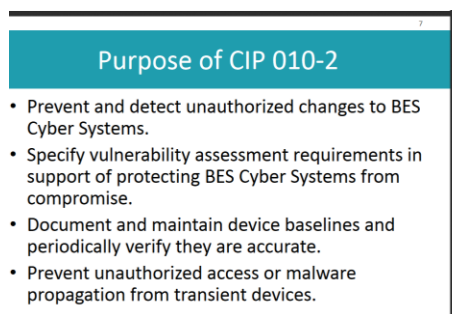
In general, we take in security vulnerability reports from our own scanning, from customers, and from vulnerability databases. Generally these are handled within our quarterly releases. We try to provide workarounds in the mean-time, however, if necessary we can do an out of band release to resolve.

Note: Refer to the link above for the document Dave is referring to.

H) CIP-010 (CIP-10/COP-010 Baseline) Cyber Security) ("Cyber Security- Configuration Change Management and Vulnerability Assessments")

- Refer to http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-2&title=Cyber%20Security%20-%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments&jurisdiction=null
- Recommend saving configs and saving Journal log entries to track config changes,.

From: <https://www.wecc.biz/Administrative/07%20-%20CIP-010-2%20-%20Christensen.pdf>



Q (per SF case 126907) Do you have a list of commands at the CLI level to pull a configuration baseline to satisfy CIP-010 compliance?

A Per Ron Dries (19 Feb 18) Taking a look at CIP-010, it does not appear to state explicitly what the configuration baseline has to be. Also this appears to be mainly a way to track device configuration and changes made to it.

<https://www.cimcor.com/blog/achieving-nerc-cip-10-compliance-with-file-integrity-monitoring>

Potentially having the customer save a configuration bundle from the SecureSync might be enough, using the saveconf command.

Keith's response to customer The Spectracom SecureSync, via its CLI interface (as well as its web browser interface) provides the means to capture and export its current configuration files and log files.

Specifically, regarding the SecureSync's configuration files, all of its configurations can be captured and exported from the unit, via its `saveconf <enter>` CLI command. Opening a connection to the CLI (via telnet and/or ssh) will generate and export a single bundle file of the unit's configurations. This file can be archived, for comparison of other config bundles, or can even be re-uploaded into the same or other SecureSyncs, as desired.

The Config files can be bundled together and downloaded via the unit's web browser in a single step. Or, the configs can first be bundled into a single file using the its `saveconf<enter>` CLI command, and then this single config bundle file can be FTP/SCP transferred out of the SecureSync's `/Home/Spectracom/Xfer/Config` directory (using a File Transfer Program, such as CoreFTP for instance).

Note that as we do periodically add to new capabilities via software updates, which may potentially add newer configurations, we typically recommend performing this `saveconf` command to extract a new config file bundle each time a new software update version has been applied. This will ensure the most recent archived file contains all applicable configuration files/settings for the software version installed.

In addition to capturing a configuration bundle using the `saveconf` command, the SecureSync maintains a "Journal.log" file, which tracks configuration changes applied to the SecureSync. The Journal log creates a new log entry for each configuration change, with an indication of which user account made the change, with which interface the change was incorporated using (such as web browser, CLI or front panel keypad) and what the configuration change was.

The Journal log entries are stored in the Journal log file inside the SecureSync. These log entries can also be optionally sent to an available syslog sever on the network for remote log file storage. The unit's logs can also be bundled together as a single log file, which can then be downloaded for archive storage. The logs can be bundled together and downloaded via the web browser in a single step. Or, the logs can first be bundled into a single file using the its `savelog <enter>` CLI command, and then FTP/SCP transferred out of the SecureSync's the `home/spectracom/xfer/log directory` (using a File Transfer Program, such as CoreFTP lite for instance).

Email from Sadie (19 Feb 2018) pertaining to WAPA NERC CIP came up when WAPA was initially validating the SecureSync. They wanted to ensure the device could be queried by their 'TripWire' systems to ensure no unauthorized changes were made and that the commands could be piped through "grep" to make sure they would get the output that they need. They asked if this command worked : `ifconfig -a | grep -a inet`

To which we confirmed,

Here is the output of the command run on a SecureSync. There is no issue for piping any authorized commands through `grep`.

```
spadmin@Spectracom ~ $ ifconfig -a | grep -a inet
inet 10.2.16.20 netmask 255.255.0.0 broadcast 10.2.255.255
inet6 fe80::76fe:48ff:fe07:ac02 prefixlen 64 scopeid 0x20<link>
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
```

CIP Baseline Testing requirements

- Refer to Salesforce cases (such as for Gerry Gasca)

I) “Services/daemons required by the vendor fo the appliance to work properly”

Based on our conference call, I believe the list below (services/daemons required for the the appliance to work properly).

Note: Please be aware that not all processes in this list below (such as the “Broadshield” option for instance) apply to all SecureSyncs- the list of services actually running in each SecureSync is likely to vary from one unit to the next.

Addlocal...Service to add a remote user (RADIUS or TACACS+) to the system for SSH login.
Apache2...HTTPS
Apache2-cert...HTTPS security certifications
Broadshield...Service to start the Broadshield software option for jamming/spoofing support
Discmond... Daemon to monitor disciplining
Fcron...Used in Linux to execute periodic command scheduling
Fcrontab...Used by Fcron to create tables in Linux
Fpaneld...Daemon to run front panel
Gbe-load... Service to load the Gigabit Ethernet driver
Gpsmond...Daemon to monitor GPS receiver
Identify...Start-up script to identify hardware in the system.
Kalarmd...Daemon for alarm monitoring and messaging.
Khtd... Daemon for managing host time system time.
Khte... Program that ensures Linux and the Timing system times agree at start up.
Kmond...Linux monitoring Daemon
Kts...Kramden Timing System (Spectracom, proprietary)
Ktslogd...Daemon for monitoring and logging KTS events.
Local...Daemon to set up scripts within Linux which are used during boot or shutdown.
Logd...Daemon for monitoring and updating logs.
Modules-load...commands used for loading/unloading modules into or out of the Linux Kernel
Net.eht0...Opens eth0 port with defaults.
Netmond...Daemon to monitor network traffic and status.
Netmount...network startup on boot
Notifyd...Daemon which handles notifications
Ntpmond...Daemon to monitor NTP.
Nwpldie... Service to discover features that are installed on startup
Nwple... Product labeling service
Pam... Linux authentication service
Perfmond...Daemon to monitor performance
Pseudod...Daemon to handle GPS information using pseudo-terminals for Broadshield
Rexd...Daemon to monitor other daemons
Snmpd...Daemon to monitor and facilitate process SNMP requests and redirect them to subserver (agents), that generate SNMP messages payload. One basic agent is integrated, the other is snmpsad
Snmpsad... Daemon to monitor and facilitate SNMP MIB. Traps.
Sql_Db...database for the Web U/I.
Sshd-create-keys...Daemon to create SSH keys for console access.
Statusd...Daemon to report system status.
Syslogd...Daemon to monitor and report syslog
Xinetd...Networking Daemon

Please let me know if there is anything else you need from us to be able to complete your CIP testing!

Thanks for identifying each of the services that are running. I assume when you say they are not “unexpected” you mean that they are required by the vendor for the appliance to work properly? If that is the case, then I think we are good on the port & services part. Please confirm this.

Going back to the conference call...we still need some guidance on how to handle the “root” and “spui” accounts. From what I remember, the accounts have passwords set that we cannot change and they have to ability to be logged into with a privilege escalated after logging into with another users shell. Our CIP requirement says that we have to “change all default passwords”. I believe we were willing to take that stance that since these accounts can’t login directly without going through the escalation of another account that we could accept that answer, however we need some way (command) to prove that the accounts only work through escalation. For instance...in our current baseline we are keying on the “/nologin” to show the other accounts that cannot log into a shell. But the “root” and “spui” have “/bin/bash” set in the passwd file. Can you help us identify a command that can prove compliance on this issue? thanks

Email Keith sent 16 Aug 2018 Thanks for your inquiry. Per your earlier requests, I now have the following information available for you from our Engineering team:

To begin, root login is blocked from remote logins (i.e.ssh).

The front panel RS-232 serial port does currently allow root login. However, we intend on changing this front panel functionality in the next SecureSync software update, so that root login won’t be available with a direct serial connection, either.

As mentioned before, when we look at the output of the local “passwd” file indicates that a Shell is available to them so that makes it appear as though we can login into them. For compliance purposes, we need to be able to provide evidence. Since we cannot change the password on root and spui, we need to be able to either prove that they cannot be logged into or show vendor documentation that the passwords were generated pseudo-randomly and are thereby unique to the device.

We need your assistance to find a command or setting in a local file to prove they cannot be logged into, or some documentation asserting that the passwords are random and unique.

A I have the following information from our Engineering team to share with you regarding the inability to login to root:

In the PAM config files. we use **pam_securetty.so** to ensure that the root account cannot be logged into.

There is a config file in SecureSyncs called **securetty** (as in “secure tty”) which lists the terminals that root is allowed to login to.

In the next SecureSync software version upgrade, this will be updated to also not allow root login from the front panel serial port.

Here is an example of the PAM login config file, with the line that uses this config file highlighted:

```
cat /etc/pam.d/login
auth include /etc/tacacs_pam.conf
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
account required pam_securetty.so
account include /etc/tacacs_pam.conf
account required pam_tally.so
account sufficient pam_unix.so
account required pam_deny.so
session include /etc/tacacs_pam.conf
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
```

session required pam_unix.so
password required pam_unix.so shadow md5

email from Keith 16 Aug 2018: Yes you are correct the securetty file is missing. This is the bug that will be resolved in the next release of software.

It was present in previous versions, and will be added back in the next software version.

As described previously the securetty file is used to describe the interfaces that root is allowed to login with.

An empty file tells the pam_securetty.so executable to not allow root to login on any interface. The next software release will add this file in.

SSH is also configured explicitly to not allow root logins.

The securetty file is what we have to indicate that root is not able to login. When that is present then the only way to access root is to login as another user and switch to the root account as we discussed previously.

Also as we discussed before spui is only accessible through the root account.

****General recommendations for vulnerability testing**

- 1) (versions prior to 5.8.9?) Disable the classic interface web browser

Email Keith sent to a customer: To disable the classic interface browser, navigate to the bottom of the Management -> Network page of the browser. At the bottom of the list of "Network Services" (left side of the page) is the "Classic UI" slider switch.



Simply slide this switch to the OFF position and the classic interface is no longer available!

Software/firmware vulnerabilities (CVEs):

- Refer to CustomerServiceassist doc for all CVEs: [..\CustomerServiceAssistance.pdf](#)

Linux/System Design vulnerabilities/limitations

- Refer to SF case 25403 (July, 2017 v5.6.0/v5.7.0)
- Refer also to JIRA-SSS-275

No.	Risk	Justification
	Severe Vulnerabilities	
1	No authentication for single user mode (lilo-linux-single-user-mode)	Access to single user mode currently requires internal physical access to the unit, including removal of the top cover, as no external connections can break into the boot process. Physical security has been considered a requirement of the end user, however, we will add password protection as a release ticket.
2	Weak permissions for Password, Shadow and Group Files (generic-passwd-shadow-group-file-permissions)	Permissions are currently as follows: -rw-r--r-- 1 root root 739 May 31 14:42 /etc/group -rw-r--r-- 1 root root 1696 May 31 14:42 /etc/passwd -rw-r----- 1 root root 726 May 31 14:42 /etc/shadow A shadow permissions setting of 640 vs 400 is required to support web UI login mechanisms with local authentication.
3	World writable files exist (unix-world-writable-files)	A few files listed as world writable, while low risk, will be marked with a release ticket to resolve. The remaining files are intended as world writable as they are intended as user configurable to support language and UI customizations available for configuration for all users.
	Moderate Vulnerabilities	
4	User home directory mode unsafe (unix-user-home-dir-mode)	This will remain as it is, so that customer can access the site to perform software upgrades. This directory requiring successful login to be able to access it, making this directory locked-down would inhibit everyone from being able to apply software updates in the field

**Email below from Paul M (excerpted from SF case 25403
SEE MY COMMENTS BELOW AFTER PEM:**

1) No authentication for single user mode (lilo-linux-single-user-mode)
PEM - We don't use LILO we use grub.

2) ICMP redirection enabled (linux-icmp-redirect)
PEM: This can be done I think. Probably beneficial.

3) No password for Grub (linux-grub-missing-passwd)
PEM: They need physical access to make use of this. If they can get to this we have issues. Doing this might complicate update???

4) Weak permissions for Password, Shadow and Group Files (generic-passwd-shadow-group-file-permissions)
PEM: They need to login so an INSIDER attack is required. WE can increase protections. Need to determine consequences.

5) World writable files exist (unix-world-writable-files)
PEM: It depends which ones they are talking about???

6) User home directory mode unsafe (unix-user-home-dir-mode)
PEM: This is needed I believe...

7) ICMP timestamp response (generic-icmp-timestamp)
PEM: We are a time server, WHY do we care that they can use ICMP to determine our time?

8) TCP timestamp response (generic-tcp-timestamp)
PEM: We are a time server, WHY do we care that they can use ICMP to determine our time?

Security Hardening: PCI-DSS / PCI compliance/PCI Audits (Payment Card Industry) Security

What is meant by our marketing material: “SecureSync is a security-hardened network appliance designed to meet rigorous network security standards and best practices”

- From: <https://www.rolia.com/products/timing-sync/enterprise-class-securesync>
- Refer to Salesforce Case 247850

Q your website states that the device is hardened according to industry standards. Do you have a document that states what that actually means? My security group is really on me about what that means. In particular this statement on your website:

A Network-centric Approach

SecureSync is a security-hardened network appliance designed to meet rigorous network security standards and best practices

Assessments/PCI DSS audits/ NERC CIP-007 and CIP-010

PCI DSS (Payment Card Industry Data Security Standard, for Credit Cards/E-Commerce)

* Our NTP time servers help customers meet **Requirement 10.4** of the PCI DSS Standards

“One aspect of PCI DSS compliance that is often overlooked – or poorly implemented – is time. Accurate time is essential to synchronize critical systems and provide the ability to correlate events and logs with a high degree of certainty.”

Inaccurate time can cause the user to be unable to access a system because the server’s certificate appears to be expired or not yet useable. Disabling the certificate check leaves servers vulnerable and could allow someone who has gained access to stay in the system indefinitely. This is also true in two-factor authentication like Google Authenticator, RSA SecurID, and others. In fact, time is such an important aspect to PCI DSS compliance that it is addressed as part of **Requirement #10, Track and Monitor All Access to Network Resources and Cardholder Data:**

10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

- 10.4.1** Critical systems have the correct and consistent time.
- 10.4.2** Time data is protected.
- 10.4.3** Time settings are received from industry-accepted time sources.

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

Available PCI DSS Reference Info for SecureSync:

A) Official PCI and general websites such as:

- https://www.pcisecuritystandards.org/document_library?category=pcidss&subcategory=pcidss_supporting#results (Select **Get Started**)
- https://www.pcisecuritystandards.org/document_library?category=pcidss&subcategory=pcidss_supporting#results (Select **Document Library**)
- https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

B) links on our Orolia website pertaining to PCI- DSS

- <https://www.orolia.com/solutions/critical-infrastructure/payment-card-industry-dss>
- https://spectracom.com/sites/default/files/document-files/PCI%20DSS%20Compliance_revB.pdf

C) SecureSync online user guide:

- http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/Conf_Def_Recom.htm?Highlight=security

D) emails and docs in:

- [I:\Customer Service\PCI \(Payment Card audits\)](I:\Customer Service\PCI (Payment Card audits))
- <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Security- Vulnerabilities -PCI compliance>
- <SecureSync\Alarms and logs\SecureSync Status and Log entries.pdf>

E) Links from Matt Loomis about this audit:

- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
- <http://spectracom.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=1851&PortalId=0>

F) Salesforce cases, such as

- 164874

“PCI AOC Attestation of Compliancy”

The AOC is a **form** used by merchants and service providers to attest to the results of a PCI DSS assessment. It is submitted to an acquirer or payment brand along with the appropriate SAQ or ROC, plus any other requested documentation.

A vulnerability scanner can detect/report PCI DSS Compliancy

This report is not an individual report of a potential vulnerability being detected. It’s reporting that the device is not PCI DSS compliant, because there are reports of potential vulnerabilities that are being detected. The unresolved/detected potential vulnerabilities are listed at the bottom of the report (under “Ports”, as shown in the example below):

21929 - PCI DSS compliance

Synopsis

Nessus has determined that this host is **NOT COMPLIANT** with the PCI DSS requirements.

Description

The remote web server is vulnerable to cross-site scripting (XSS) attacks, implements old SSL2.0 cryptography, runs obsolete software dangerous vulnerabilities (CVSS base score == 4).

If you are conducting this scan through the Nessus Remote Service Plugin, and if you disagree with the results, you may submit this Scanlet for PCI Validator and dispute the findings through our web interface.

See Also

<http://www.pcisecuritystandards.org>
http://www.orolia.com/sites/default/files/document-files/PCI_DSS

Risk Factor

High

Plugin Information:

Publication date: 2008/09/07, Modification date: 2012/04/27

Ports

tcp:80

+ 3 medium risk flaws were found. See 1
<https://www.sshnet.com/pipermail/sshnet-pkg/201004/0419181.html>
<https://www.sshnet.com/pipermail/sshnet-pkg/201004/0419182.html>
<https://www.sshnet.com/pipermail/sshnet-pkg/201004/0419183.html>

26220 - TCP/IP Timestamps Supported

In this example, items 58751, 57582 and 51192 are detected potential vulnerabilities. Clearing these items will allow this report to be automatically cleared

In this example, items 58751, 57582 and 51192 are detected potential vulnerabilities. Clearing these items will allow this report to be automatically cleared

info on Services/daemons running in SecureSync

- refer to (in this doc): [User accounts](#)

Info on Accounts (root/spui/spfactory/spadmin)

- refer to (in this doc): [User accounts](#)
-

logging requirements for PCI-DSS compliancy:

- Refer to Salesforce cases such as 164874
- Here are few links on our website on PCI-DSS.
<https://spectracom.com/customsearch?nocache=1528288286&searchText=PCI+DSS&offset=0>

Q (from customer) Is there a reference document available that details the log data from SecureSync? Basically I need to know the mapping of event IDs to events so we can have our Log Management system send alerts on specific log entries?

Email from Morgan to Apps Engineering We have some questions on our support of the PCI-DSS (???) standards on the SecureSync product. Can you provide input to their concern and our support of the standard?

<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

A (6 Jun 18) email from Sylvain to Morgan You can also reassure your customer that we have customers who has purchased especially the SecureSync for PCI DSS audit process (mandatory for them) and they succeeded.
https://spectracom.com/sites/default/files/document-files/PCI%20DSS%20Compliance_revB.pdf

Request for information on sample log entries/details for all possible SecureSync log entries

- Refer to “**Status and Logs**” tech note : [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Alarms and logs\SecureSync Status and Log entries.pdf](#)
- Refer also to info (in this doc): [Logs](#)

below info is From SF case 164874

Two sections that would contain the information I need don't have example entries in the doc. System Log and Journal Log. Here's the PCI requirements we're trying to map to.

- Access to sensitive and critical data (10.2.1)
- Action taken by user with administrative or root privileges (10.2.2)
- Invalid logical access attempts (I.e. Access denied) (10.2.4)
- Successful and Unsuccessful logons and logoffs (10.2.4)
 - o I found these in the Auth Log
- Startup and shutdown of system logs (10.2.3)
- Gaps in security event logs (10.2.3)
- Create, modify or delete system level objects (10.2.7)
- Attempts to access security relevant files, utilities, security profiles, password configurations (10.2.4)
- Invalid attempts to security relevant files, utilities, security profiles, and passwords configurations (10.2.4)
- Passwords resets (10.2.5)
- Data modifications or deletion using commands or special scripts executed outside of normal application functionality by technical users (10.2.7)
- Code modifications (10.2.7)
- Modification, additions or deletion of application and operating system configurations (10.2.7)
- Recovery attempts
- Use of compilers
- System Software installations
- Attempt to change system clocks (10.4.1)

ISO 8601 (ISO-8601) compliancy (internationally accepted way to represent dates and times)

- ISO 8601 describes an internationally accepted way to represent dates and times using numbers.
- Refer to Custservice assistance document for more info
- ISO 8601 tackles this uncertainty (of using various methods to indicate date/time) by setting out an internationally agreed way to represent dates: YYYY-MM-DD

SecureSyncs/9400s

- **Web browser date/time display:** does use this particular formatting
- **Front panel date/time display:** does not use this particular formatting
- **ASCII output:** Formats 0, 1, 2 and 3 do not use this particular formatting
- **NTP/PTP:** does not use this particular formatting
- **Syslog logs:** (per Dave S, The syslog timestamps that are in our logs are not ISO 8601 compliant)

To begin, the SecureSync can display and outputs time/date info in several places/ways, such as on the front panel, in its web browser, in the units logs. via NTP and also via various optional Option Cards that can be installed to receive and or/output date/time using various methods (PTP, ASCII, IRIG, Havequick, etc).

The SecureSync's web browser reported date format is compliant with ISO 8601. But the vast majority of outputs available from the SecureSync are not ISO 8601 compliant. So I would recommend indicating in the survey you received that the SecureSync isn't ISO 8601 compliant (note that many of these limitations are due to the protocols that SecureSync supports and not a limitation of the SecureSync itself).

IEC 60945 (Maritime Navigation and Radiocommunication Equipment and Systems)

Corrosion, shock and vibe, etc

- Refer to Salesforce Case 247953
- Refer to "IEC 60945" in [..\CustomerServiceAssistance.pdf](#)
- Refer to "1902-188N" *environmental test report) [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Mechanical - environmental \(shock-vibe. IEC 60945\)\Maritime-Corrosion testing \(IEC 60945\)](#)
- As of at least Sept 2020, we apparently do not specify anything about "IEC 60945" in SecureSync literature

My summary of the info further below (my understanding)

- We tested the 1200 SecureSyncs against IEC 60945, but apparently didn't get Certification
- We tested just one base configuration (**1200-213**) and just Option Card configuration of SecureSync against IEC 60945.
- Test report (1902-187E) and associated EMI report to IEC 60945-2002 (1902-188N) obtained from Tom Richardson are both at: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Mechanical - environmental \(shock-vibe. IEC 60945\)\Maritime-Corrosion testing \(IEC 60945\)](#)

Email from Tom Richardson (2 Oct 2020) (pertaining to Salesforce Case 247953)

Hi Keith,

We did do IEC 60945 testing on the 1200. See attached report. We haven't done the 2400 yet. We tested a model 1200-213 and the units are similar enough that that should be representative of the entire model. You should explain to the customer about our configuration process.

I think they are referring to section 8.12, Corrosion (salt mist) (all equipment categories) of the standard. Post Test Inspection showed some signs of rust and erosion. Mainly the small screws had rust on them. When disassembled, the unit showed a small amount of salt coming in from the back where the small holes are. The unit powered up and functioned properly. See page 38 to 43 of the report.

Thank you for the info you sent, it has been very helpful. We have reviewed it and have a couple further questions I was hoping you could help us answer.

- 1) Is it possible to get a letter for the corrosion section of IEC 60945?
- 2) Has there been any EMC/EMI testing done on these units, preferably 60945 but if not any EMC/EMI info would be helpful.
- 3) Has there been any certification on the option cards that are able to be installed in the base units?
- 4) Is there a way to generate a Part number/order code that can be used to order a base model with options installed in specific slots?

Associated Reply from Tom Richardson (14 Oct 2020)

For item 1. I am assuming they would like a Declaration of Conformity but the one we have is really just for CE. Maybe some sort of declaration of compliance.

For item 2. I'm sorry Keith I should have included the EMI report to IEC 60945-2002 also.

For item 3. We only tested the one configuration to 60945. I think it would be representative of the product.

Associated Reply from Emmanuel (15 Oct 2020)

Dear all,

I suggest you ask OSI if they are looking for a certification letter coming from a Certification Body (which we cannot provide) or if a declaration letter, referring to our test report and claiming compliance to the appropriate section of 60945, would be acceptable.

If the latter is acceptable, then could Tom or Justin write such statement ?

IEC 61850 (electrical substation automation specifications)

- Refer to "IEC 61850" in [..\CustomerServiceAssistance.pdf](#)

Voluntary Product Accessibility Template (VPAT)”.Section 508 form / Form 508 of The Rehabilitation Act (for people with disabilities: Blind, hearing impaired. etc)

- The form is called “Voluntary Product Accessibility Template (VPAT)”.
- refer also to “Voluntary Product Accessibility Template (VPAT)” in: [..\CustomerServiceAssistance.pdf](#)
- Refer to Salesforce Cases such as 208201

Q What is Section 508 compliance?

A In 1998 the US Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. **Section 508** was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals.

We claim exception from this form:

Email from Sadie Nedo (11 Sept 2019) We do not have a VPAT. We take the following exception to Section 508: Exception in 1194.3 (f) applies to our products:

(f) Products located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment are not required to comply with this part.

Japanese Safety compliance (RoHs/UL94HB/ Inorganic phosphorus/ESD tolerance data or ESD level)

- Refer to SF case 120838

Email from TOYO: Our customer Mitsubishi informed us that they would like to know the following information For their safety standard policy.

Model : 1200-xyz unit and 1204-xx module
UL94HB level (V2,V1,V0,5VB,5VA)
ESD IEC61000-4-2 level (1,2,3,4,x)
Included Inorganic phosphorus

Reply from Josh (~ 30 Oct 17) We had to go through safety reviews by Japanese Safety Authority sometime ago for our SecureSync. Kindly get with Yamanouchi-san for those documents that we submitted back then and let me know what else is missing for Mitsubishi please.

Q They require the below system. 1200-033 x 1 (1204-19 x 1, 1204-11 x 1)

A Email from Josh to TOYO (21 Oct 2019) Please note our responses below :

RoHS : 1204-11 assembly meets RoHS3

UL94HB level (V2,V1,V0,5VB,5VA) :

- Board is 94-V0, Safety 60950-1, 62368-1.
- PCB is 94V0.

Inorganic phosphorus : We do not use Inorganic phosphorus in our boards.

ESD tolerance data or ESD level : 1204-11 meet IEC/EN 61000-4-2.

"Indian Trusted Telecom Portal"

- Refer to Salesforce Case 286800 (July 2022)
- Refer to sites such as: <https://dot.gov.in/accessservices/trusted-telecom-portal-policy-regarding-input-data-pertaining-non-india-registered>

Scada Systems

Refer to sites such as: <http://www.cimation.com/blog/bid/190307/What-is-SCADA-Anyway>

SCADA is the system responsible for monitoring a technical process and, in some cases, controlling and optimizing those processes. Through these systems, human operators monitor and control input and output values related to safe and efficient operations from one central location, regularly acquiring data that allows supervision of industrial controls in real (or near real) time.

Terms

- **SCADA Stands for:** Supervisory Control and Data Acquisition (SCADA)
- **HMI:** Human Machine Interfaces
- **Points / Data Points** To the application developer the network represents itself as a set of elementary data elements, called data points (or simply points). These data points are the logical representation of the underlying physical process, which control network nodes drive or measure. Each node can be associated with one or more data points. In the logical view each data point represents a single datum of the application. It can correspond to an aspect of the real world (such as a certain room temperature or the state of a switch) or be of more abstract nature (e.g., a temperature set point). The data points are connected through a directed graph, distinguishing output points and input points. The application is defined by this graph and a set of processing rules describing the interactions caused by the change of a point value. The logical links which this graph defines can be entirely different from the physical connections between the nodes.

Y2K38 (year 2038 rollover) (“Unix Millennium Bug”)

- Refer to “Y2k38” in the Custserviceassistance document

Lafayette (Model 1200 series SecureSync)



Links/Shortcuts:

- **Shortcut to SecureSync manual (1200-5000-0050) in Arena:** https://app.bom.com/items/detail-attach?item_id=1203165562&version_id=10364984008&orb_msg_single_search_p=1&redirect_seqno=7336157236
- **Shortcut to Harris SecureSync manual (1200-5000-H050) in Arena** https://app.bom.com/items/detail-attach?item_id=1210695099&version_id=10356765578&orb_msg_single_search_p=1&redirect_seqno=7336161513
- Shortcut to SAASM receiver Manual Addendum (1200-5000-0056)

Note: NOT in Arena as it's a FOUO document: <U:\Documentation\Released\Manuals\1200-xxxx-xxxx>

Note: Upload to customer using ARMDEC website: <https://safe.amrdec.army.mil/safe/>

- **Shortcut to the SecureSync Service Manual (1200-5000-0056) not yet in Arena:** <I:\New Released\Manuals\1200-xxxx-xxxx>

Please Note: The Service manual is not to be sent to customers/dealers

- **Shortcut to SecureSync data sheet:** <https://oroliagroup.sharepoint.com/sites/oroliasalesmarketing/>
 - **Shortcut to firmware upgrades:** [PSB, PSP software updates\948x](#) and [SecureSync\948x](#) and [SecureSync Software updates](#)
 - **Shortcut to SecureSync Product Service bulletins:** [PSB, PSP software updates\948x](#) and [SecureSync\Securesync Product Service Bulletins](#)
 - **Shortcut to pre-release candidate software updates:** <S:\Engineering\Projects\Lafayette\200 Engineering Documents\Working Files\Releases>
 - **Shortcut to Engineering design Projects/test plans for SecureSync:** <S:\Engineering\Projects\Lafayette>
 - **Link to manual CD that we ship (1217-5003-0001) in Arena:** https://app.bom.com/items/detail-bom-flat?item_id=1202847112&version_id=10228803588&nested_bom_p=0
- Manual CD includes manuals/quick start guides for 814x product, 9300 and 9400 series, TimeView display clocks, CTCSS and SecureSync

Email from Scott Zmuda (18 June 2020) If you are not already aware of all of these links, here they are. Good to share with customer from time to time. Just a refresher.

Quick Start Guide

<https://www.rolia.com/documents/quickstart-guide-securesync>

User Manual

<https://www.rolia.com/documents/user-reference-guide-securesync-time-and-frequency-synchronization-system>

Online User Manual

<http://manuals.spectracom.com/SS/>

Online User Manual - Troubleshooting

<http://manuals.spectracom.com/SS/Content/NC and SS/Com/Topics/TROUBLE/>

Antenna Installation Guide

<https://www.orolia.com/documents/antenna-installation-guide-model-8230-and-8320aj>

Surge Suppressor Installation Guide

<https://www.orolia.com/documents/installation-guide-model-8226-gps-antenna-sure-suppressor>

In-Line Amplifier Installation Guide

<https://www.orolia.com/documents/installation-guide-model-8227-gps-inline-amplifier>

Troubleshooting GNSS reception

<https://www.orolia.com/documents/troubleshooting-gpsglonass-reception-securesync>

Option Card Installation Guide

<https://www.orolia.com/documents/option-card-installation-guide-securesync>

SecureSync Support

<https://www.orolia.com/support/spectracom/securesync-and-netclock-9400-support>

Support Bulletins

<https://support.spectracom.com/support-bulletins/securesync>

Last Time Buy (LTB) / End of Life (EOL) / Discontinuance of 1200 SecureSyncs

- Note this section is for 1200 SecureSyncs only. NetClock 9400s have their own section in this doc (towards the end) for their associated info with end of life.
- 1200 SecureSync EOL letter (May 2022) excerpted below and located in: [!:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\1- End of Life \(EOL\)](!:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\1- End of Life (EOL))

May 4th, 2022

SecureSync 1200 Discontinuance and Last Time Buy Notification - **UPDATED**

Dear valued customer and partner,

Due to recent changes in our supply chain environment, we had to revisit and update this SecureSync 1200 discontinuance and Last Time Buy Notification. Changes, versus the April initial issuance, are noted in **bold** characters.

This notice is to inform you of the pending discontinuance of the SecureSync 1200 time and frequency reference system. The SecureSync 1200 is succeeded by the next generation enhanced **SecureSync 2400** which is available today .

This discontinuance notice applies to all SecureSync 1200 base units (Part Number starting with 1200) and to a limited number of option cards and accessories. A detailed list is provided in appendix.

A Last Time Buy opportunity will be offered with following terms:

- **LTB orders will be accepted immediately**
- Shipments of LTB orders can be scheduled in to end 2023

Due to limited part availability, orders will be honored only while supply is available.

SecureSync 1200 technical support will be provided up to end of 2030. During the support period :

- Premium Support service contracts can be renewed
- Hardware repairs will be available based on component availability
- Software updates will be provided to support critical bugs and security vulnerabilities on an ad-hoc basis

Orolia encourages customers to migrate to the next generation SecureSync platform. SecureSync 2400 brings a range of improvements associated with networking, processing power, security and monitorability, while maintaining the flexibility and modularity that was part of SecureSync 1200. In addition, SecureSync 2400 offers more built-in outputs along with hot-swap power supplies for improved availability. Orolia's Application Engineering team is available to guide you through the transition from SecureSync 1200 to SecureSync 2400.

At Orolia, we provide our customers with the most resilient Position, Navigation, and Timing solutions and we continue to optimize our products by integrating the latest technology, leading the way to improved performances and capabilities.

Please feel free to contact your Orolia sales representative or myself for any additional information you would need.

Sincerely,
Emmanuel SICSIK-PARE
Strategic Product Manager,

Appendix

Discontinued Part Numbers

Part Number Comment

All SecureSync 1200 base units

P/N following the scheme :

1200-xyz

A-1200-xyz

1200-wxyz-abcd

A-1200-wxyz-abcd

Option Cards which are not supported on SS2400

1204-06 – 3 Gb Ethernet

1204-3B – Gb Slave PTP

1204-1A – GB-GRAM SAASM

1204-49/4A to be selected with SecureSync 2400

1204-50, with M-code capability, to be selected with SecureSync 2400

Accessories not supported on SS2400

PS06R-2Z1M-DT01 – Power Supply option

1200-0000-0704 – ancillary kit rugged install

1200-0000-0711 – ancillary mounting kit AC

1200-0000-0712 - ancillary mounting kit DC

SecureSync Tech Brief: 1200 SecureSync to 2400 SecureSync Migration Guide

Refer to our website: https://www.rolia.com/wp-content/uploads/2022/03/SecureSync-1200-to-2400-Migration-Guide_US_03-02-22.pdf

Schematics/ Component Part Numbers

- Schematic for SecureSync **main** PCB board (1200-1001-0200) (in 1200-0000-F001) in Arena: https://app.bom.com/files/detail-summary?file_master_id=1240372444&file_id=1754447396
- Schematic for SecureSync **front panel** PCB board (1200-1001-0300) (in 1200-0000-F004) in Arena: https://app.bom.com/items/detail-spec?item_id=1202839909&version_id=10259851368&orb_msg_single_search_p=1&redirect_seqno=5835050934

Component Part Numbers:

- P/N for the main SecureSync PCB board: 1200-0013-2000

Note: Per Jen Sanza- See Dave West to order a replacement PCB board.

Spectracom Product roadmaps

Refer to Emmanuel's Product Roadmaps at: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\Spectracom Product roadmap>

International shipping/Export control (ECCN, CCATS and HTS codes) for SecureSyncs and NetClock 9400s

CCATS HTS and ECCN Numbers for all our products

- Refer to the "Export Control" section of the custserviceassist doc: <..\CustomerServiceAssistance.pdf>
- For CCATS, refer also to "CCATS Numbers" Section in the Custserviceassist doc: <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>
- Refer also to the latest version of the "US_Export_Controls_Matrix" (or order info in SAP)
<I:\Trade Compliance\Export Control Matrix>
<I:\Customer Service\Export Control-HTS and ECCN numbers>

A) (NO SAASM receiver installed, and no ITAR Specials installed)

(Non-ITAR variants of SecureSync)

- US HTS code is 8471.80.9000
- ECCN is now 5A991b (as of Oct, 2016. Used to be 5A002.a.1. See note in red further below)
- CCATS for 9483/9489 (not SecureSync) is G400623 (See note in red further below)
 - CCATS for non-ITAR SecureSyncs (no SAASM/No ITAR Specials) – we do not have one (See note in red further below)

Per Dave Sohn (26 May 2021) We do not have a specific CCATS against SecureSync 1200. We are self-certifying

our 1200 ECCN determination based on CCATS G170373 completed against NetClock 9483/9489.

Per Mary Slack (29 Jan 2018) Per Mary Slack (29 Jan 18) If a customer requests a **CCATS** (*Commodity Classification Automated Tracking System – an official classification determination by the US Department of Commerce*) for one of our products, you may go to this folder location to get one – if we have it: <I:\Trade Compliance\CCATS Commerce Classifications>. Go ahead and bookmark the page.

Also found in that folder are two letters regarding our self-classification of SecureSync (one for Hong Kong specifically), and one regarding our self-classification of GSG-55.

If a customer requests a CCATS for a product but you don't see it in that folder, please let me know. Either I neglected to put it in the folder, or more likely, we self-classified. If a self-classification letter for a specific product is required, as opposed to you telling them we self-classified, then let me know the product and I'll write one up.

- Note: Regarding “letter of explanation” mentioned in email below, refer to the two docs at: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Intl Shipping - ECCN and HTS codes>

Q We have semi-annual encryption reporting requirements and our corporate offices are requesting the CCATS number for this product. I need the CCATS number or confirmation that one does not exist. I need this information to Corporate by 2:00PM EST Monday 29 January 2018. Thank you for your prompt attention to this matter.

A From Keith 29 Jan KW (after talking to Mary Slack, mod from DLs earlier email below

To begin, all of the SecureSync Serial Numbers referenced are Spectracom Model Number 1200-033 (indicating they do not have a SAASM GPS receiver installed). As there is no SAASM receiver (nor any ITAR-controlled Specials) installed in these SecureSyncs, this variant of SecureSync is not ITAR-Controlled.

FYI: The ECCN for non-ITAR controlled SecureSyncs changed (back in October, 2017) due to export control reform, from 5A002 to 5A991. We do not have a CCATS Number for non-ITAR variants of SecureSync, because we self-classified our equipment after this classification change.

However, we do have a CCATS Number for the Spectracom NetClock Models 9483/9489, which I've attached. These Model NetClocks (which are also non-ITAR controlled devices) are very similar to the non-ITAR variants of the SecureSync.

Also attached you should find a Letter of Explanation for the info above.

Earlier Email from Dave L (19 Apr 2017) I have a correction to the ECCN for Securesync. It is now 5A991.

The ECCN for SecureSync changed due to export control reform from 5A002 to 5A991 in October. We do not have a CCATS, because we self-classified our equipment after the classification change. However, we do have a CCATS for 9483/9489, which I've attached.

We have provided a letter of explanation.

B) With SAASM receiver installed/ITAR Specials

- **ITAR variants of SecureSync**
- **US HTS code: 8471.80.0000**
- **Europe HTS code: 8471.80.0000**
- **ECCN Number: XII(d)(2)(ii)**

Repairs/SAASM RMAs

Zeli Systems

Email Wade sent to a customer Hi, thank you for the quick response. We ship to Zeli Systems because they can receive our product with the integrated SAASM receiver. Zeli Systems strips out the SAASM receiver and ships the unit minus the SAASM receiver to our Orolia USA manufacturing facility here in Rochester, NY. It's our facility here that will actually do the evaluation and repair of the unit. Once repaired then it will be shipped back to Zeli Systems where the SAASM receiver is reinstalled and operationally verified then sent back to you.

The Cage code for Orolia USA is 59797, Zeli Systems Cage Code is 1HCL1

OGSI Supported Products

Email from Scott Zmuda (13 Oct 2020) Team – Anything with an “A” in the serial number and or product number is a special OGSI build and should be forwarded to support@oroliads.com (585.250.1545)
Orolia USA should not attempt to troubleshoot or support until evaluated and requested by OGSI.

Example: Per Salesforce Case 248890 “We have never heard of this model number **A-1228-1310**. I believe it must be a OGSI product.”

Just FYI:

Comment from Keith I thought the number “A-1228” sounded familiar. A quick search of Salesforce shows its apparently associated with VersaPNTs.

MTBF/MTTR

SecureSync MTBF/MTTR

- Refer to the MTBF/MTTR section in [..\CustomerServiceAssistance.pdf](#)

Rear panel/Slots-Slot Numbering

C) SecureSync rear panel

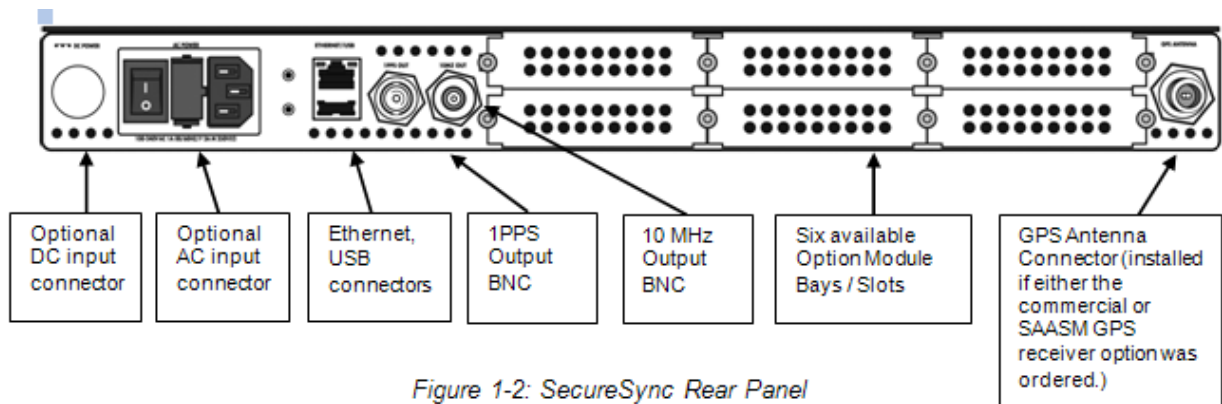


Figure 1-2: SecureSync Rear Panel

D) Model 9483 rear panel



E) Slot numbers for both SecureSync and 9483



In-house SecureSync references for Engineering

Do not change configs without talking to Dave Sohn/Paul Myers!!!

- 1) House Reference **IP address:** 10.10.10.2 (internal use only)
- 2) For Engineering use only (not on Internet)

[HTTPS://time.spectracomcorp.com](https://time.spectracomcorp.com) (**IP address:** 74.112.39.70) Hostname: Spectracom

Username: spadmin

Password: Spadmin3

- Oscillator installed: Low Phase Noise RB Note: reported as "OCXO (1ppb)"
- Option cards installed: 10 MHz out, 1PPS out, PTP, IRIG-out-1204-05, 1204-06

SecureSyncs/Model 9483s on the Internet (outside of firewall)

Note: The 2 Sales units reside in the Rack in engineering and are controlled by the IT department.

A) SecureSync on Internet for Sales demo:

- This unit resides in the Rack in engineering and is controlled by the IT department.
- IP address= <https://66.193.84.103>

HTTP is disabled, so to get into the browser, type <https://66.193.84.103>

Option Cards this unit should have installed: 1204-1C (1PPS out) and 1204-12 (10/100 PTP)
Oscillator installed: OCXO
See Linda McCormick for granting customer access to these Sales demo units

User account for customers to login

- **Username:** salesdemo
- **Password:** SSdemo1234

Note: Per Paul Myers- don't give out this spadmin login password (below). Instead, create a user account (user rights) on the unit that the customer can use to access the browser.

Admin account

Username: **spadmin**

Password: **SPadmin4** (SP in caps - rest in lower-case letters)

B) SecureSync on Internet for Sales demo:

- This unit resides in the Rack in engineering and is controlled by the IT department.

IP address= 63.138.60.57 HTTP is disabled, so to get into the browser, type <HTTPS://63.138.60.57> or <HTTPS://time.spectracomcorp.com>

Option Cards should have installed: 1204-06 Gb Ethernet
Oscillator: OCXO (1ppb)

The correct login for the Model 9483/SecureSync is:

User account for customers

Username: **spadmin**

Password: **SPadmin3** (SP in caps - rest in lower-case letters)

Note: Per Paul Myers- don't give out this login password. Create a user account on the unit that the customer can use to access the browser.

Factory and spadmin

Visio Stencils/shapes

Link to the Visio graphic file referenced below: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Visio](#)

Email from Morgan (2 Feb 16) Thank you for the questions about the Visio Stencils. We do have some (5) available, these have not been updated since 2013. Review the link below to see if we have what you need. We do have CAD drawings.
<https://spectracom.com/documents/secsync-visio-shapes>

Email from Tim Klimasewski to a customer (22 Apr 2013) We do not have any visios built using our SecureSync, but I can share with you the attached portable network graphic file that I have used as a simple illustration. You can insert it into a visio document (or even any of our product photos from the web site) if you are looking for something generic. If you are looking for back panel detail to show connections, then you may need to create it yourself.

Data sheet /Specs

- Direct link to SecureSync datasheet on our website: <https://www.rolia.com/sites/default/files/document-files/SecureSync%20Standard%20005-29-20.pdf>

“factory default secured and hardened”

- Refer to Salesforce Case 247850

Q “On your website you state that this device is factory default secured and hardened. My security team would like to know what this actually means.”

A: “What the statement **security-hardened** means to Orolia is that we provide the ability of disabling insecure protocols and having capabilities out of the box with support for things like RADIUS, LDAP, TACACS+. This allows the customer to enable the security parameter dictated by their organization.”

Lafayette Main Board/Chassis Hardware Specification

- Refer to

https://spectracom.atlassian.net/wiki/spaces/DMND/pages/255787009/4in1+Option+Card?preview=/255787009/332201997/LAF-202-F%20Lafayette%20Main%20Board%20Chassis%20HW%20Spec%201_0.doc

Lafayette Main Board/Chassis HW Spec.
Security Level: SPECTRACOM PROPRIETARY
Audience: INTERNAL

Date: July 13, 2009
Document Number: LAF-202-F
Revision: 1.0

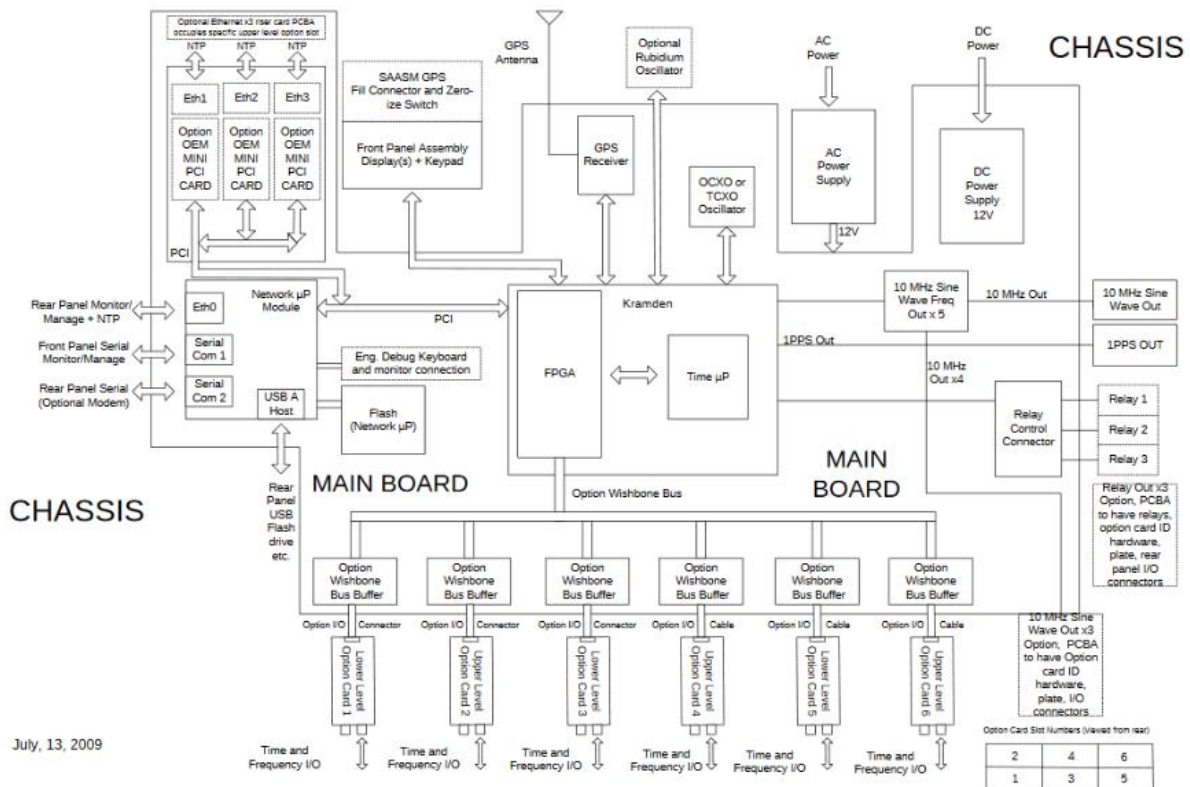


Figure 1 – Lafayette System diagram

**IP rating (Ingress Protection)

- Refer to the “IP rating/Ingress Protection rating” section in the Custserviceassistance document.

“One sigma” for the 1PPS specs (standard deviation)

- Based on the “three-sigma rule”
- Refer to sites such as:

http://en.wikipedia.org/wiki/Standard_deviation

http://en.wikipedia.org/wiki/68%E2%80%9395%E2%80%9399.7_rule

<http://math.stackexchange.com/questions/320370/how-to-calculate-standard-deviation-and-use-three-sigma-rule-for-couple-variable>

Sigma	Certainty	expected frequency outside of range
1 sigma	66.7%	1 in 3
2 sigma	95%	1 in 22
3 sigma	99%	1 in 370

In [statistics](#), the **standard deviation (SD)** (represented by the Greek letter sigma, σ) is a measure that is used to quantify the amount of variation or [dispersion](#) of a set of data values.^[1] A standard deviation close to 0 indicates that the data points tend to be very close to the [mean](#) (also called the expected value) of the set, while a high standard deviation indicates that the data points are spread out over a wider range of values.

In [statistics](#), the so-called **68–95–99.7 rule** is a shorthand used to remember the percentage of values that lie within a band around the [mean](#) in a [normal distribution](#) with a width of one, two and three [standard deviations](#), respectively; more accurately, 68.27%, 95.45% and 99.73% of the values lie within one, two and three standard deviations of the mean,

In the [empirical sciences](#) the so-called **three-sigma rule of thumb** expresses a conventional heuristic that "nearly all" values are taken to lie within three standard deviations of the mean, i.e. that it is empirically useful to treat 99.7% probability as "near certainty"

Mechanical (shock, vibe) / Environmental testing/Safety-MSDS (Hazardous material)

Chassis dimensions/correct width

Chassis measurements (from the S/S datasheet)

see the note below this excerpt

Physical & Environmental

Size/Weight:

- Designed for EIA 19" rack.
16.75" W x 1.72" H (1U) x 14.0" D actual
(425 mm W x 44 mm H x 356 mm D actual)
- Weight: 6.5 lbs. (3 kg)
- Rack mount hardware included (assembly required)

Note: The Chassis width is slightly incorrect on the datasheet (found Jan, 2018)

- Refer to SF case 125054
- SecureSync's datasheet indicates width is **16.75 inches**. But the actual width (per the mechanical drawings of the chassis/cover) is **16.5354 inches**.
 - Don't know for sure, but I suspect the measurement on the datasheet was simply rounded-up for simplicity.

Chassis/top cover screws

Top cover screws

- Our P/N for the screws **HM20-03R5-0406** (in Arena) https://app.bom.com/items/detail-spec?item_id=1202842961&version_id=10221212998
 - **The Top cover screws are:** M3-5,18-8SS,6MM, BLACK OXIDE

Email from Scott Zmuda (24 Oct 2019) regarding removing/reinstalling cover screws

The SecureSync Top Cover screws was an interesting conversation today and I wanted to make sure we were all on the same page when speaking with customers about this and in regards to the CF card replacement.

We all know that these screws can be a challenge and can potentially strip or snap off when removing. The fact that there is 20 of these screws is difficult enough. So a few points I would like all of us to remember. Regardless of what metal they are made of or the strength of the screw itself, we certainly do want to send the message to our customers that these screws are inferior or poor quality. We should stay aware from discussing Tencel strength or hardness of the metal when dealing with customers. We always want to ensure we promote our products and discuss them in the most positive way as possible. Even though this may be challenging at times, it is best for us, our customers and our business to speak positively about our products. Positive but honest.

In regards to the top cover screws, here are some key points to use if and when you discuss with a customer (I thank Tom Ellison for this insight):

- 1) Orolia recommends a Phillips #1 head to use for removal and replacement of the top cover screws
- 2) Problems with damaging these screws are typically caused by using an improper size bit such as a Phillips #2 or by using a bit that is worn and rounded at the head. Again, we recommend using a Phillips #1 in good or new condition.
- 3) We should also recommend a light tap on the screw driver at first contact to the screw to assist in releasing the paint bond between it and the cover itself. It aids in the removal of the screws.
- 4) If for whatever reason customers are still having issues and perhaps have destroyed screws in the process, we can certainly provide spare screws along with the CF cards. It's a great show of support and minor cost to ensure our customers are supported and satisfied.

Q A piece of feedback from the field engineer is as below.
Do you sell proprietary chassis cover screws, or could we use generic ones for PC build?

Can't open anymore the chassis cover due to 3 of the screws have already stripped or damage heads. For now we are able to manage to install the card on slot 5 because it was installed on bottom slot, and besides slot 4 and 6 are still empty which can be open to help you see and examine the installed card if properly seated.

A reply from Dave L (10 Oct 17) The cover screws are common size Flat Head M3.5 6mm black oxide finish and you can probably find them anywhere locally.

Removing stripped cover screws can be done but they are small so care must be taken to avoid damaging them too much to be removed. The trick is to rotate them counterclockwise by tapping a punch or small flathead screwdriver or a chisel to make them turn out.

You may also be able to get a small flathead screwdriver to grab in what is left of the screws slots and get it to turn. Using a dremel tool to cut a slot in the screw head is a good method if you have one.
And of course drilling the head off the screw will allow you to remove the cover and then maybe turn out the screw with pliers.

This video may help: <https://www.youtube.com/watch?v=mTFQbaT3Zc> Hopefully in the future you will never have to change any option cards.

Clear chromate coating on bottom of chassis/MIL-DTL-5541

➤ Refer to Salesforce case 180339

per <https://en.wikipedia.org/wiki/MIL-DTL-5541>

MIL-DTL-5541: The **MIL-DTL-5541** specification covers chemical conversion coatings that form protective coatings by chemical reaction with aluminum and aluminum alloy; these coatings are categorized by the following types and classes.

Q The bottom of the enclosure is plated with clear chromate. Is that done according to MIL-DTL-5541 or other standard?

A Reply from Morgan (3 Dec 2018) Currently we only specify RoHS compliance for clear chromate plating on our aluminum fabricated parts.

1200-1000-0709 (Empty Option Bay slot covers)

➤ For purchase of replacement slot covers: Refer to our Online Store (<https://store.rolia.com/>)

Environmental info (Mercury, lead, asbestos, plastics) / Hazardous material (Rb material)

Conflict Minerals report

- Refer to the “Conflict Minerals” folder in the Customer Service drive: <I:\Customer Service\Conflict minerals report> (note this folder may contain docs for other products- not just SecureSync. Make sure to select the appropriate documents).

Asbestos (1200 SecureSyncs only)

- Refer to Salesforce Case 218627 (in “files”, see “

Per Emmanuel (24 May 2023)

But you will find below answering elements

Actually, we just need to confirm that we meet CE Mark, per our declaration of conformity. This CE mark compliance embeds compliance to ROHS and REACH regulations, that all our products meet. Asbestos are part of substance list covered by REACH.

For US, toxic substances, as covered by Toxic Substances Control Act, and including :

- * TSCA Section 6(h) Toxic Substances Control Act
- * PFAS (Per- and polyfluoroalkyl Substances)

Are also included in the list of REACH-related substances, and are therefore covered by our Declaration of Conformity.

Emmanuel SICSIK-PARE
Strategic Product Manager | Safran Trusted 4D

MSDS info

Hazardous materials/Rubidium material

A) Coin Battery for RTC (all SecureSyncs and 9400 NetClocks)

- Refer to the following:
 - <..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement\lithium battery>
 - <https://industrial.panasonic.com/ww/products/batteries/primary-batteries/lithium-batteries/coin-type-lithium-batteries-br-series/BR3032>

B) SpectraTime Rb material (when Rb oscillator is installed)

- Refer to the Spectratime PSDS (“Spectratime hazmat331.pdf”) on our website at:
<http://support.spectracom.com/articles/FAQ/Security-sheet-integrated-Spectratime-Rubidium-parts?retURL=%2Fapex%2FknowledgeSiteHome&popup=false>
- Refer also to the great webpage for info on Rb including health risks/measures:
<http://www.lennotech.com/periodic/elements/rb.htm>

C) Lithium battery in GB-Gram SAASM receiver (if this receiver is installed)

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement\Battery for SAASM receiver> (links to the “US only” drive)

Mercury, lead, Rohs

Q. Any Mercury contained in the system such as LCD?

A Per Keith after talking with Dave Sohn The LCD display is RoHS compliant. We are not aware of it (nor the rest of the SecureSync) containing any mercury.

Q Any other hazardous materials such as Lead, RoHS complaint?

Keith's response: The SecureSync is RoHS compliant. Also, the 1200-233 has a SpectraTime Rubidium oscillator installed. Attached you should find a PSDS Safety Data Sheet associated with this Rubidium oscillator.

Q Any specific safety warnings for operation and maintenance?

Keith's response: Maintenance of the SecureSync in the field is really limited to the installation or removal of any Option Cards, which requires power be removed from the SecureSync and standard ESD practices be followed.

PVC Plastics

➤ Any PVC plastics or electrical insulation?

A Wire/cable PVC insulation.

Huawei as a supplier of parts for SecureSyncs/NetClocks

➤ Refer to Salesforce Case 239378

Q. "Do the Spectracom SecureSync NTP appliances contain components from Huawei"

A. Reply from Morgan Randolph (15 July 2020) Per Tom Richardson and PLM, the answer is no Huawei.

A. Reply from Ryan Johnson (15 July 2020) Hi Keith, I confirm that from a design perspective, we have not designed in anything with Huawei as a supplier.

Shock/vibe (MIL-STD-810F)

- For shock/vibe of antennas (such as Model 8230s), refer to <..\CustomerServiceAssistance.pdf>
- Refer also to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Mechanical - environmental>

SecureSync has been shock/vibe tested against MIL-STD-810F

- Refer to the SecureSync datasheet for specs

Email from Dave Sohn (30 Sept 2019) We've found an error in our datasheet that occurred during one of our previous updates, as it relates to our vibration testing. We are going to be updating our datasheet, which should now state:

	Operating	Storage	MIL-STD-810F
Vibration	10-55Hz/0.07g, 55-500Hz/1.0g	10-55Hz/0.15g, 55-500Hz/2.0g	514.5

Engineers associated with shock/vibe testing

Slightly modified Reply from Tom Richardson (26 Sept 2019) when I requested additional data from our Shock/vibe test: "Including Randy (Randolf.Zingo@orolia.com) and Nigel (nigel.ramoutar@orolia.com) in this discussion. Any mechanical testing was either done by them or Scott Holmes"

Note: The documents that Scott references in his emails below can be found at: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Mechanical - environmental>

Email from Scott Holmes to Sam Otto (29 Apr 2013) The vibration testing was performed at a test lab with calibrated vibration and sensing equipment. The SecureSync was attached to a fixture very similar to an equipment rack. We used both front and back attachment points to anchor the SecureSync to the rack. I have attached is the certificate for that testing in case that's helpful.

Email from Dave Sohn (18 Feb 2013) SecureSync mechanical/environmental specifications use testing methods according to MIL-STD-810F. Scott Holmes can provide more detail on that.

Follow-up email from Scott Holmes (18 Feb 2013) Attached is a Certificate of Test for the shock and vibration testing we did, using methods according to MIL-STD-810F, that lists the limits and values we tested the product to. There were no failures.

The last page of the SecureSync Specification sheet (attached also), under 'Environmental', shows the reference paragraphs we followed in MIL-STD-810F for the testing performed.

Temperature testing was done here at Spectracom but we did not create a certificate for that.

Humidity and Altitude tests were not performed, but we stand by these values based on product performance in the field.

FAQs regarding Shock/vibe

Q I got your message about the sinusoidal and the 0.07Grms. Thanks for getting back to me. The Grms unit indicates random vibration, so I guess I am still a bit confused. Was this a spec that you tested to, was it a destructive test?

I guess I should state my concern. We have a couple of these products and are planning on putting them into a mobile environment. I am looking for the most information you can give me, that way I can compare your specs to my specs to see if a mobile environment would be acceptable for you product.

A Reply from Morgan (22 Sept 2015) We vibration tested the SecureSync to a specific profile for a customer at the time of development. The limits of the profile are indicated on our spec without too much information on the customers profile as part of the NDA. The final installation was a naval shipboard environment. We have not tested the SecureSync to any other mobile environment up to this point.

Data sheet indicates “0.07g”

Q I am wondering if the “0.07g” was referring to sinusoidal vibration or root-mean-squared vibration from a random vibration test.

A Reply from Scott Holmes to Morgan (10 Sept 15) it's in RMS.

Data sheet indicates “0.53oz”

Q. On the spec sheet for the 1200-027 it references an operating shock limit of “15g/0.53oz, 11ms, half sine wave” and vibration limit of “10-55Hz/0.07g, 55-500Hz/1.0g”. I am wondering what was meant by including the “0.53oz” in the shock limit.

A From Scott Holmes to Morgan (10 Sept 15) This came up 8 or 10 months ago. It's a conversion from grams to oz. ☺
The unit of mass (grams) and the unit of g-force both have the same symbol (g), so someone misinterpreted this when they did the data sheet years ago and it was not noticed until recently. It should say - operating shock limit of “15g, 11ms, half sine wave”

Does 10-55Hz/0.07g” and “55-500”/1.0g” in Data sheet refer to PSD /ASD curve break points

Q Also, in the stated shock and vibration limits, on the data sheet. You reference “10-55Hz/0.07g” and “55-500”/1.0g”. You mentioned before that this was a random test. Thus, do those values refer to PSD / ASD curve break points? Should they have units of g²/Hz?

A Reply from Morgan (7 Oct 15) The 10 to 55Hz and the 55-500Hz tests were run separately. There were no break points in the profiles. Yes, the data sheets need to be updated and the units should be in g²/Hz

Shock/vibe testing for Option Cards

Q We are using two different configurations of SecureSync, 1200-027 and a 1200-227. With modules 1204-05 and 1204-01. I was wondering if the stated shock and vibe specs in the environmental section of the SecureSync Time and Frequency Synchronization Platform data sheet reference tests of just the platform, or were the modules installed during the shock and vibe tests?

Also, in the stated shock and vibration limits, on the data sheet. You reference “10-55Hz/0.07g” and “55-500”/1.0g”. You mentioned before that this was a random test. Thus, do those values refer to PSD / ASD curve break points? Should they have units of g²/Hz?

Is it possible to send me the test report, or really any information would help, on the shock and vibration testing?

A Reply from Morgan (7 Oct 2015): We ran the test with all the option card slots occupied by the cards that were developed and released at the time (2010). We did not have a 1PPS card installed (1204-01) so that card has not been tested for shock and vibration.

***Telcordia GR-63-CORE (NEBS Earthquake/seismic-related enclosures)

Refer to sites such as: <http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=082705147D000542&KEYWORDS=&TITLE=&DOCUMENT=GR-63&DATE=&CLASS=&COUNT=1000>

Telecordia: NEBS (telecom) requirements for Physical Protection:

- Criteria for equipment cooling air-inlet and exhaust locations are revised and clarified.
- Operating temperature test conditions are now a function of the equipment-cooling air-inlet location.
- A detailed heat dissipation calculation procedure is provided for frame and shelf-level equipment.
- Fire resistance test methods are updated to address specific service provider requirements.

Email from Morgan (6 June 16, referring to Scott Holmes) I spoke and forward your email to Scott our mechanical engineer and he said, that we have not done any formal or informal testing for the seismic standard Telcordia GR-63-CORE.

If you have this requirement, we can research this and give you a quote for cost. We have done this in the past for customers that require special testing.

“Zones” of earthquake testing (such as Zone 5, Zone 4, etc)

- Per Tim Tetreault (from his email further below)
 - Zone 5 Earthquake testing is the worst case testing.
 - Zone 4 Earthquake would be “pretty rough”.

Testing which has been performed on our equipment (such as for Specials)

Email from Tim Tetrault to Dave Sohn (7 Nov 2018) about Specials testing that has been performed

We did 2 sets of seismic testing. One on the AMDR chassis and one on the QEWR which was the 20" chassis. At the time, we wanted to be conservative so we ruggedized the 20" chassis. We RTV'd components and added a stiffening plate inside. We also used the full length rack ears that run the length of the chassis. We only had to do testing for the easiest of the zones. Zone 1.

In the email below, it calls out zone 4. Zone 5 is the worst so 4 would be pretty rough. It also gets worse if it is installed in a rack. The higher up in the rack, the worse the force can be. So for that application, I would recommend the chassis be ruggedized, similar to what we did in the ARL-E project.

The email doesn't reference any standards for the seismic testing. This testing can be run differently depending on what the customer wants. Do they wanted tested per GR-63-CORE?

For the QEWR project, we only needed to operate through the seismic event, and meet spec once the event was done. Do we need to meet spec through the seismic event? Phase Noise? I see below that there is an operational vibration spec. Do we know what spec's we need to meet during the vibration?

CCATS Number for SecureSync

- Refer to “CCATS Numbers” Section in the Custserviceassist doc: <..\CustomerServiceAssistance.pdf>

ECAT DS (ECATS) Number for SecureSync

Q. Also, is there an ECAT DS number for the recommended antenna/cable for the 9483?

A. (from Will Hickey, 9 Mar 16) The ECATS P/N for the 9483 is: DS948305

1200 SecureSync Model Numbering scheme

Model 1200- A B C

A is Input Power

0= AC only
1= AC + (10-17vdc)
2= AC + (21-60vdc)
3= (10-17vdc) only
4= (21-60vdc) only
5= AC input, 12vdc out

B is Oscillator

0= TCXO
1= Standard OCXO (5PPB)
2= Low Phase Noise OCXO (1PPB)
3= Standard Rubidium (.5ppb)
5= Low Phase Noise Rubidium (.1ppb)
6= SRO-100 Rb, LPN OCXO and external
Wenzel High G oscillator
7= Wenzel Low-G 10 MHz-SC Citrine
Crystal Oscillator (P/N Y100R-0002-
PC02) for Hughes SecureSync

C is GPS receiver

1= No GPS receiver installed
3= uBlox, Res-SMT-GG or Res-T (commercial receiver)
5= Trimble Force 22 SAASM receiver
7= GB-Gram SAASM receiver
9= M-Code SecureSync GPS module

For edit purposes

A is Input Power

0= AC only
1= AC + (10-17vdc)
2= AC + (21-60vdc)
3= (10-17vdc) only
4= (21-60vdc) only
5= AC input, 12vdc out

B is Oscillator

0= TCXO
1= Standard OCXO (5PPB)
2= Low Phase Noise OCXO (1PPB)
3= Standard Rubidium (.5ppb)
5= Low Phase Noise Rubidium (.1ppb)
6= SRO-100 Rb, LPN OCXO and external
Wenzel High G oscillator
7= Wenzel Low-G 10 MHz-SC Citrine
Crystal Oscillator (P/N Y100R-0002-
PC02) for Hughes SecureSync

C is GPS receiver

1= No GPS receiver installed
3= uBlox, Res-SMT-GG or Res-T (commercial receiver)
5= Trimble Force 22 SAASM receiver
7= GB-Gram SAASM receiver
9= M-Code SecureSync GPS module

Fault tolerance

- Fault Tolerance is limited. Faults on input references will transition unit into Holdover mode.

Enterprise-level Network Monitoring Tools (NMS)/ NRPE (such as Nagios, Zabbix Cacti, Splunk Integration, QRadar, etc, Xi Epoch by Nutanix)

- Network Monitoring Systems (NMS) and Network Security Management platforms are tools for monitoring network devices.
- Some example NMS systems include Solarwinds, HP OpenView, Nagios, libreNMS, Zabbix and Cacti
- Refer also to the “Enterprise-level network monitoring tools” Section in the custserviceassistance doc for more info. I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf
- SecureSync/9400 series: As of at least software v5.5.1 (Jan 2017), SecureSync/9400 does not have any of these NMS systems installed, as needed for full compatibility (Denis Reilly was looking into this for future implementations).
 - But SecureSync does support SNMP, which is typically supported with the NMS systems (resulting in a partial compatibility with NMS systems)

BMS / IBMS (Building Management System / Integrated Building Management Systems)

- BMS and IBMS appear to be generic terms for various monitoring systems installed in a building.
“Integrated BMS is the key to 'intelligent buildings', equipped with a variety of monitoring devices and control systems, both automated and manned. Together they help regulate a long array of building services and utilities.”

Note: The REST API may be supported and helpful for customers using these various NMS tools

SIEM devices

- Refer to Salesforce Case 232269

Your question

Does your product support sending information to a **SIEM** device

My response (reply from Keith 13 May 2020)

This is the first time I've ever had this question asked about the SecureSync...

I am not familiar with SIEM devices, so I searched a bit online about it (didn't find too much).

This appears to be a part of an NMS System? If it is, most NMS system support basic monitoring capabilities that SecureSync also supports (such as general SNMP and syslog remote logging capabilities).

But many NMS systems require special software modules be installed in the network devices being monitored, for enhanced monitoring. The SecureSync does not have any of these modules installed and doesn't permit users being able to install these custom modules. When monitoring the SecureSync with an NMS requiring custom software modules be installed, its sometimes necessary to identify the SecureSync in the NMs that it doesn't support custom-enhanced monitoring.

If the SIEM device can operate as a standard syslog server (for remote logging storage), or if its supports standard SNMP functionality, for alert notifications/remote monitoring, SecureSyncs support these capabilities. But if they require any specialized interface (software modules and/or hardware), the SecureSyncs do not have this capability available.

FYI: In case you weren't already aware of it being available, a great source of source of info (the most up-to-date info and very easily searched) for the SecureSync is the online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INTRO/Getting_Started.htm

For instance, if they support syslogging, please refer to:

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/Logs_Configuring.htm?Highlight=syslog

For information about SNMP monitoring, refer to: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Intro.htm

In case SIEM devices only interface with specially designed inputs/outputs, I am forwarding your inquiry over to our SecureSync Product Manger for his consideration of a potential add of this feature to SecureSyncs, in the future! Many of our added product capabilities over the years have been directly due to questions such as this!!!

Examples of some available Network Monitoring tools/Network Security tools

A) HP OpenView (NNMi)

- Refer to [I:\Customer Service\NMS-NNMI \(network monitoring\)\HP OpenView-NNMI](I:\Customer Service\NMS-NNMI (network monitoring)\HP OpenView-NNMI)

Network Node Manager i (NNMi) is a program that helps a network administrator view and manage the conditions in a computer network. NNMi is part of the OpenView suite of enterprise system management applications from HPE (Hewlett-Packard Enterprise), the company's business products and services division.

Note: Not yet known if the REST API is supported, but may be helpful if it is supported.

Example Unique OID numbers: .1.3.6.1.4.11.2.17.19.2.2.2

Need to configure OpenView not to use NNMI with SecureSyncs

(from the NNMI deployment guide at the link above)

NNMI does not perform any out-of-the-box discovery. You must configure discovery before any devices appear in the NNMI topology.

Each discovered node counts toward the license limit, regardless of whether NNMI is actively managing that node. The capacity of your NNMI license might influence your approach to discovery.

Status monitoring considerations might also influence your choices. By default, the State Poller only monitors interfaces connected to devices NNMI has discovered. You can override this default for some areas of your network, and you can discover the devices beyond the edge of your responsibility. (For information on the State Poller, see [NNMI State Polling](#) on page 65.)

NNMI provides two primary discovery configuration models:

- **List-based discovery**—Explicitly tell NNMI exactly which devices should be added to the database and monitored through a list of seeds.
- **Rule-based discovery**—Tell NNMI which areas of your network and device types should be added to the database, give NNMI a starting address in each area, and then let NNMI discover the defined devices.

You can use any combination of list-based and rule-based discovery to configure what NNMI should discover. Initial discovery adds these devices to the NNMI topology, and then spiral discovery routinely rediscovers the network to ensure that the topology remains current.

B) Solarwinds Network Performance Monitor (NPM)

Email from Mark Reeves with airbus (13 Apr 15) Thanks for opening up the dialogue. I am not sure if NCM will work without NPM Solarwind's Network Performance Monitor. If you already have NPM then this will plug right into it as evaluation software. If you don't then we will have to figure out how to get over that hurdle. I could also get you remote access to my Lab Network where I have both installed. I also have a Spectracom Unit in my Lab as well. Let me know what your thoughts are. I left the info for my Solarwinds contact in the email below.

NCM 7.3.2

<http://downloads.solarwinds.com/solarwinds/Release/OrionNCM/SolarWinds-NCM-v7.3.2-Eval.zip>

Note: Not yet known if the REST API is supported, but may be helpful if it is supported.

C) Nagios software

- At least version 5.9.5 and below are not compatible with this program and there are no plans at this time to add support for it.
- Open Source software for monitoring network devices which support Nagios.
- Refer to sites such as: <http://www.nagios.org/>
- (Jan 2015) Per Denis Reilly- We are aware of Nagios and would like to one day be able to support the plug-ins for this software with SecureSync . It's "on our radar", but not likely to support it anytime soon.

Note: Not yet known if the REST API is supported, but may be helpful if it is supported.

NRPE (Nagios Remote Plugin Executor)

- As of at least version 5.4.5, we don't currently support/have plans to integrate NRPE
- For info on NRPE, refer to sites such as <https://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details>

"NRPE allows you to remotely execute Nagios plugins on other Linux/Unix machines. This allows you to monitor remote machine metrics (disk usage, CPU load, etc.). NRPE can also communicate with some of the Windows agent addons, so you can execute scripts and check metrics on remote Windows machines as well."

Two Emails from Dave Sohn (5 Aug 16) Thank you for your inquiry about utilizing Nagios to monitor the product. We don't currently have plans for integrating NRPE within the product, but we have been doing some integration with Nagios both with standard plugins, and some beta custom plugins for specific elements. What additional information are you looking to monitor as they may be available through

another means besides NRPE? Thanks.

Below is a snapshot of one of our similar products, SecureSync, being monitored by Nagios using SNMP and other plugins (including some beta custom plugins from Spectracom). The SNMP plugins we used are from <https://sourceforge.net/projects/nagios-snmp/>. Is this the type of information you are referring to? The CPU line is for cpu % usage, but I believe there is an option to get the 1/5/15 minute values instead.

Current Networ
Last Updated: Fri A
Updated every 90 s
Nagios® Core™ 4.1
Logged in as nagios

[View History For TI](#)
[View Notifications F](#)

D) Xi Epoch by Nutanix

- Refer to <https://www.nutanix.com/blog/introducing-xi-epoch-by-nutanix>

E) Zabbix software

- **Note:** Not yet known if the REST API is supported, but may be helpful if it is supported.

F) Cacti software

- At least version 5.5.1 and below are not compatible with this program and there are no plans at this time to add support for it.
- Refer to sites such as <http://www.cacti.net/>
- Cacti is a complete network graphing solution designed to harness the power of [RRDTool](#)'s data storage and graphing functionality. Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features out of the box. All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices.
- (Jan 2015) Per Denis Reilly- He isn't familiar with this tool. Not sure if we'll ever support it in the future with products such as SecureSync.

Note: Not yet known if the REST API is supported, but may be helpful if it is supported.

G) Splunk Integration

- At least version 5.5.1 and below are not compatible with this program and there are no plans at this time to add support for it.
- Request to support this in SecureSync- Refer to Salesforce case 24342
- For info, refer to sites such as: <http://www.snaplogic.com/solutions/splunk-integration>
- **REST API:** Splunk provides a fully-documented and supported REST API with over 200 endpoints. Developers can programmatically index, search, and visualize data in Splunk from any application.

H) IBM QRadar (Network Security Management platform)

Note: Not yet known if the REST API is supported, but may be helpful if it is supported.

- At least version 5.5.1 and below are not compatible with this program and there are no plans at this time to add support for it.
- Refer to sites such as: <http://www.itsecurity.com/?s=12699> and <http://www-03.ibm.com/software/products/en/qradar-siem/>
- Request to support this in SecureSync- Refer to Salesforce case 24342

IBM® QRadar® SIEM consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. It normalizes and correlates raw data to identify security offenses, and uses an advanced Sense Analytics engine to baseline normal behavior, detect anomalies, uncover advanced threats, and remove false positives. As an option, this software incorporates IBM X-Force® Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. IBM QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

QRadar (tm) is a network security management platform that provides situational awareness and compliance support to organizations that need to tighten security and improve regulatory compliance with a modest investment in time and resources.

Surveillance: It combines flow-based network knowledge, security event correlation and asset-based vulnerability assessment to provide unmatched coverage of security events and network behavior in one console.

Analysis: QRadar's Judicial System Logic relates this data to policy violations, network misuse and threats to business assets. It tracks offenses against a business asset and gathers all the security incidents and network activity in an offense profile.

Control: QRadar leverages the most appropriate security device or infrastructure component to resolve offenses. It offers multiple options for remediation to fix the problem from the console.

Bomgar/Lieberman Software (aka “Lieberman tool”, “Liebsoft”) Privileged Access Management (PAM)

- Refer to Salesforce case 171498

from <https://www.bomgar.com/blog/entry/lieberman-software-acquired>

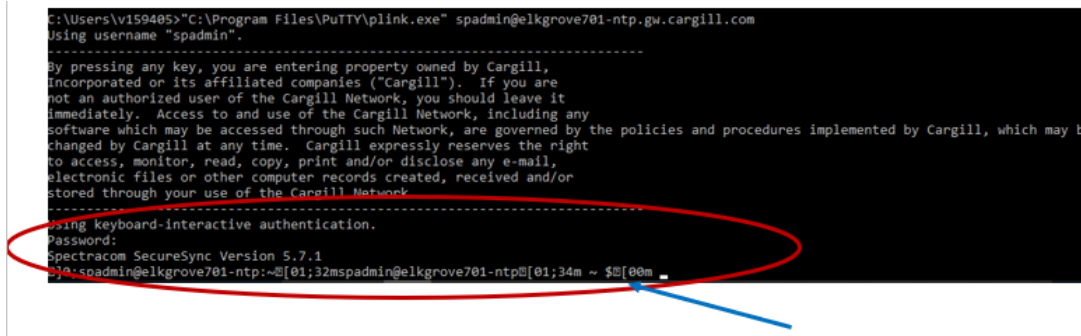
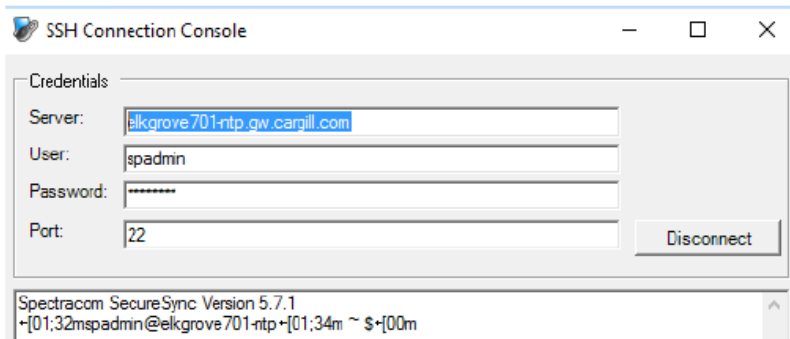
In the Privileged Access Management (PAM) market, buyers are seeking products that not only improve security and accountability, but also don't impede their users in their day to day job tasks. Offering privileged session management and credential management as a solution from one company means that customers can streamline their PAM implementations while addressing a wide variety of use cases related to access and passwords.

“Post login, it prompts with weird characters”

- See the circle/arrow in the 2nd screenshot below for an example
- Per Ron Fries -The issue appears to be due to terminal colors, and the terminal they are using is not able to handle them.
- For example: <https://unix.stackexchange.com/questions/143684/what-is-the-problem-with-the-output-of-plink>

Customer Report (Aug 2018) We have SecureSync setup in our environment and we are integrating its local account password management to Lieberman tool. In pursuing doing this integration we are failing to change the password of the accounts and below is the update from the tools team. Please share your advice to get this integrated to Lieberman tool for its password management.

Post login, it prompts with weird characters. It may be due to color coding or character length limitation. Please check with vendor.



Email from Ron Dries (21 Aug 18) The software version is 5.7.1 and they are using ssh as spadmin. The issue appears to be due to terminal colors, and the terminal they are using is not able to handle them.

For example: <https://unix.stackexchange.com/questions/143684/what-is-the-problem-with-the-output-of-plink>

I started to look into the Lieberman tool, and there might be an option to emulate a terminal. Can we have them try to set the terminal type and see if that improves it?

Excerpt from the Lieberman Tool installation guide:

“Terminal Type - Name of terminal to emulate (xterm, linux, scoansi, att6386, sun, aixterm, vt220, vt100, ansi, vt52, xterm-color, linux-lat, at386, vt320, vt102 and tn6530-8).”

I think the built-in terminal is not able to handle the terminal color commands.

Hi Michael,

Good day to you! I hope all is going well!

Thanks for submitting a new Case on the Orolia/Spectracom website and for your great question pertaining to SecureSyncs.

Your question

Does your product support sending information to a **SIEM** device

My response

This is the first time I've ever had this question asked about the SecureSync...

I am not familiar with the SIEM devices, so I searched a bit online about it (didn't find too much).

If this device can operate as a standard syslog server (for remote logging storage), or if it supports standard SNMP functionality for alert notifications/remote monitoring, SecureSyncs support these capabilities. But if they require any specialized interface (software and/or hardware), the SecureSyncs do not have this capability available.

FYI: In case you weren't already aware of it being available, a great source of source of info (the most up-to-date info and very easily searched) for the SecureSync is the online SecureSync user guide at:

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INTRO/Getting_Started.htm

For instance, if they support syslogging, please refer to:

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/Logs_Configuring.htm?Highlight=syslog

For information about SNMP monitoring, refer to:

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Intro.htm?

In case SIEM devices only interface with specially designed inputs/outputs, I am forwarding your inquiry over to our SecureSync Product Manger for his consideration of a potential add of this feature to SecureSyncs, in the future! Many of our added product capabilities over the years have been directly due to questions such as this!!!

Veritas NetBackup (“OS NetBackup”)

- At least version 5.5.1 and below are not compatible with this program and there are no plans at this time to add support for it.
- Refer to sites such as <https://en.wikipedia.org/wiki/NetBackup>

Veritas NetBackup (earlier **Symantec** NetBackup) is an enterprise level **heterogeneous backup** and recovery suite. It provides cross-platform backup functionality to a large variety of **Windows**, **UNIX** and **Linux** operating systems.

It is set up with a central master **server** that manages both media servers (containing the backup media) and clients. Core server platforms are, **Solaris**, **HP-UX**, **AIX**, **Tru64**, **Linux** and **Windows**.

Q Email from Dave L to Dave Sohn (2 May 26) hyundai-autoever asked if we could have SecureSync OS Netbackup.

A Reply from Dave Sohn (2 May 16) We haven't designed any support for NetBackup, although I'm not that familiar with the mechanisms. As such, it isn't included on our roadmap either.

False alerts due to NMS/NNMi being enabled in the SNMP manager

Find out the associated OID and see if it's a valid SecureSync OID. If not, its probably due to a NNMI monitoring,

1) Virtual and physical memory has insufficient capacity or malfunctioning

➤ Refer to SF case 25091 for example

Report from, Danny Loke: Our customer had reported that one of their securesync Virtual and physical memory has insufficient capacity or malfunctioning. The unit is still functioning as normal, front display panel is OK as well. Their unit is running V5.3.0.

```
[10].1.3.6.1.4.1.11.2.17.19.2.2.10 (Integer): 1
[11].1.3.6.1.4.1.11.2.17.19.2.2.11 (OctetString): Memory on
NC2NTP01 has insufficient capacity or is malfunctioning
```

EMAIL FROM Keith To Ron Dries: The response below in red is regarding Salesforce case 25091. I briefly mentioned it to you last week (my belief they were monitoring it with HP OpenView with NNMI enabled- resulting in a false repor of "Virtual and physical memory has insufficient capacity or malfunctioning." - was correct)".

Hi Keith,

Reply from customer:

I have confirmed we are able to disable the OID for NNMI monitoring only, but do get back to us the reviews of your Application engineer for us to be sure there is no real memory issues in our NTP server.

Per my recommendation, they have now disabled NNMI for the SecureSync, but are still concerned they may have "bad memory". Do we have a way for them to see the memory is fine? We have OIDs for reporting amounts of memory. But I'm not aware of reporting memory is good or bad.

MEMORY:	
Total Swap Size:	.1.3.6.1.4.1.2021.4.3.0
Available Swap Space:	.1.3.6.1.4.1.2021.4.4.0
Total RAM in machine:	.1.3.6.1.4.1.2021.4.5.0
Total RAM used:	.1.3.6.1.4.1.2021.4.6.0
Total RAM Free:	.1.3.6.1.4.1.2021.4.11.0
Total RAM Shared:	.1.3.6.1.4.1.2021.4.13.0
Total RAM Buffered:	.1.3.6.1.4.1.2021.4.14.0
Total Cached Memory:	.1.3.6.1.4.1.2021.4.15.0

Thanks,

Email from Keith I wanted to give you a status update regarding your SecureSync customer receiving NMS alerts of possible bad memory.

I think I have a pretty good idea on what is happening here, though I am confirming this with our Applications engineer. The two directly related OIDs that your customer provided you appear to be unique to the NNMI plug-in module, and are not Spectracom SecureSync-supported OIDs. What I can say for sure is that the Spectracom does not currently contain/support NNMI plug-in module data. This module is special software that needs to be integrated into the SecureSync's software in order to be able to respond to these unique objects.

The SecureSync only supports the Spectracom MIBs and some generic MIBs (such as the RFC-1213 MIBS). The SecureSync can't respond to other objects that are unique to the NNMI module. our SecureSync is not responding at all to either of these objects. Since I wasn't sure what they even were, I googled them and found them in a guide for the NNMI module, which explains why I wasn't seeing a response to them. Since the SecureSync is not responding to these objects, it appears their NMS may be incorrectly handling the "no reply" to the objects, resulting in false alerts being asserted, Even while I am confirming this info with the Engineer, you can go ahead and let your customer know that if their NMS system has

configuration available to enable/disable NNMI for each device its monitoring, they should disable NNMI for the SecureSync(s), since the SecureSync does not support this functionally. I highly suspect this will then prevent the false alerts from being asserted. I will get back to you, with any additional info I receive from the engineer, once he has reviewed it!

Another email from Keith to BetaIT (18 Jul 17) I am responding for Eric. Since I have only run across this condition once (maybe twice), it's highly likely he may not have ever seen this condition before (especially since its highly likely not a true alert condition)!

Your customer is likely monitoring the SecureSync using an SNMP/NMS Manager (such as HP OpenView for instance) which has NNMI monitoring enabled for the address of the SecureSync. NNMI monitoring consists of very specialized SNMP OID numbers which require the network device being monitored (such as the SecureSync in this case) to have a special plug-in module installed, which adds the ability to support NNMI monitoring. the SecureSync does not have a NNMI plug0in module installed, and therefore does not support this function.

NMS software which supports NNMI monitoring should have "per-device" configuration available which allows NNMI monitoring to be disabled by IP Address/hostname, for all of the devices on the network which don't support this very specialized monitoring (your customer should treat the SecureSync as another workstation on the network, as standard Windows workstations don't typically support NNMI monitoring, either). Trying to use NNMI to monitor a network device which doesn't support this unique function results in false alerts being generated by the NMS software.

The specific example of this that I saw was with HP OpenView NMS software. They too were seeing this exact same alert, as shown below. HP OpenVew software does have the ability to disable NNMI monitoring per each network device its monitoring, and this customer was able to disable NNMI for the SecureSync, preventing OpenView from sending this false/errant alert.

Ethernet Monitor page and graphs

A) Eth0 only

Tools -> Ethernet Monitor page (added in software update version 5.4.0)

- Eth0 transmit/receive graphs are in the Tools -> Ethernet Monitor page
- This new page was added in update v5.4.0



Versions 5.4.5 and above- Ethernet Monitor now correctly downloads graph in excel spreadsheet file

- Update software version 5.4.5 now correctly downloads graph in Excel spreadsheet file.

B) Ethernet loading data for Eth0, as well as Eth1, Eth2 and Eth3 (when 1204-06 Gb card is installed)

- Sqlite database ("log_eth_mons" table) reports ethernet throughput (received/transmit)

sys_timestamp	eth0_rx_bytes	eth0_tx_bytes	rx_bytes_per_sec	tx_bytes_per_sec	eth1_rx_bytes	eth1_tx_bytes	rx_byt ^
filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
:017-07-12 2...	0	0	0	0	72067907	85269044	63
:017-07-12 2...	0	0	0	0	72073434	85271833	90

CPU Free memory and CPU usage/utilization (and System Monitor page)

CPU usage knowledge base article: <http://support.spectracom.com/articles/FAQ/Reported-CPU-usage?q=processor&>

KTS Timing system microprocessor (U1)

- - the “inner” processor - CPU usage not available via either CLI or web browser.
 - **KTS processor (U1)** is for running the timing system.
 - **ETX module:** Outward (“external”) CPU usage can be read via CLI commands such as the “top” command or SNMP (not reported in the web browser).
 - ETX module is used with SNMP, NTP (one of the higher priorities in the system), Apache web browser, oscillator disciplining, alarm monitoring and notifications, front panel, GPS monitor, etc (items that are displayed in the “**top**” and “**rc-status**” cli commands

Q. With the software upgrade to version 5.0.2, we are seeing CPU at 90%. Is this a normal condition for 5.0.2? On the one we have only rebooted but not upgraded, I am running CPU at 31%, memory at 22%

A. The reported processor usage for the processor that can report this information (the one for the Operating System) is running at about 90%. But the NTP server is an embedded system with the reported usage being from the “outward” processor and not the one that runs the majority of functions inside the unit.

The “outward” processor that can report usage is just for the OS, including the web browser functionality and the daemons that are running. The rest of the core functionality of the NTP server (such as inputs/outputs, Option Cards, etc) is all controlled by a separate processor that doesn't report its usage.

If you have several users logged into the web browser at the same time, the reported usage will increase. But this doesn't affect the other processor that is running everything else. If you want to minimize the reported usage of the OS Micro, we just recommend minimizing the number of users simultaneously logged into the web browser.

Tools -> System Monitor page (added in software version 5.3.1)

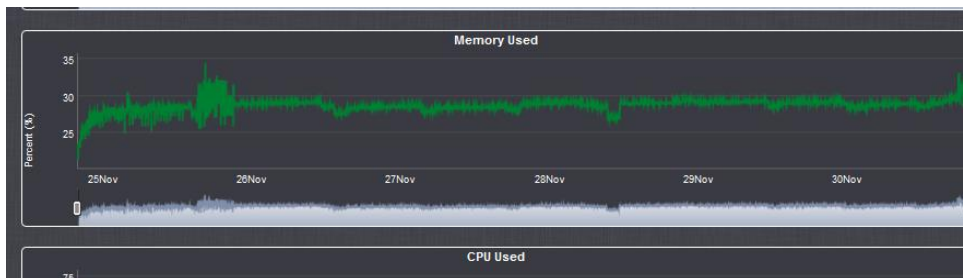
- Memory and CPU usage graphs and the Tools -> System Monitor page were added in v5.3.1

CPU free memory (ETX module - “outer CPU”)

- Refer to <http://www.binarytides.com/linux-command-check-memory-usage/>
- Free memory can be read/viewed via various methods, including a graph in the browser (starting in v5.3.1), via CLI commands or via SNMP

1. Memory Used” graph at the bottom of the Tools -> System Monitor page of the newer browser

- This graph available starting in software update version 5.3.1



Details of this graph

Partial email from Tim Hammer (24 Sept 2021) Memory Used is determined using data obtained from the Linux kernel and represents the percentage of memory that is not available on demand. During the course of operations, applications (functionality) will use memory, and potentially more memory the longer an

application runs. In addition, the kernel will utilize some memory to improve system performance. Normal operations will result in fluctuations, including periods of growth in the memory used. As applications and the kernel complete operations or identify memory usage that is no longer required, the amount of memory used will decrease.
(RE: "available on demand" – the memory utilized by the kernel to improve system performance can/will be relinquished to meet the need of an application)

Memory used graph is showing high memory usage (software issue)

Q This customer is seeing high CPU usage and he is concerned (note: it was around 80% with v5.3.1 installed)

A (from Dave Sohn, 29 Feb 16, referring to at least version 5.3.1 and likely v5.4.0) This may just be a reporting issue. The graph isn't taking into account freeable memory. That means that less memory is actually in use than is shown in the graph. That memory has not been freed by the system yet, so is still counted as used. Have them run a "free -m" command to provide us with the memory information as well to check. We are fixing the graph reporting for future versions.

2. Reading the "outer" processor memory stats via CLI (telnet/SSH or serial)

- Can use CLI commands such as "**top**", "**free**", "**free -m**", "**cat proc/meminfo**" or "**vmstat**" to read the CPU's free memory
 - Note that **free**, **top** and **vmstat** all report the same memory values

3. **top** command via CLI to retrieve the CPU memory usage is a standard linux command (need to use the entire phrase)

Refer to http://linux.about.com/od/commands/l/blcmdl1_top.htm

```
top - 13:58:52 up 15:40,  1 user,  load average: 1.13, 1.20, 1.33
Tasks: 73 total,  1 running, 72 sleeping,  0 stopped,  0 zombie
%Cpu(s): 41.6 us, 25.0 sy,  0.0 ni, 30.7 id,  2.5 wa,  0.0 hi,  0.1 si,  0.0 st
KiB Mem:  505944 total, 140644 used, 365300 free,  21424 buffers
KiB Swap:    0 total,    0 used,    0 free.  62740 cached Mem
```

"CPU" associated fields

us: Time spent running non-kernel code. (user time, including nice time)

sy: Time spent running kernel code. (system time)

id: Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time. (**Note: CPU usage is the inverse of this value. So if the idle is 15, the usage is 85%**)

wa: Time spent waiting for IO. Prior to Linux 2.5.41, shown as zero.

Note: "free memory" also consists of memory that is placed in buffers and in cache, as this memory can be made freeable at any time, as required. Unlike other commands that also report memory (such as "free -m"). "top" doesn't report all freeable memory as a single numerical value. The freeable memory in cache and in buffers are reported separately in the top command. To get the full amount of freeable memory, need to add together the "**free**", "**buffers**" and "**cached Mem**" (as highlighted above). Freeable memory is the total.

Note that if you just watch "**free**" by itself, this value may decrease over time, making it appear that a memory leak is occurring. But when adding all three values together, the result should remain fairly constant over time.

- Starting in software update version 5.0.0, the Linux OS (Gentoo) grabs as much available RAM memory as possible and holds it until memory is requested. It then releases memory as needed. It is completely normal/expected for free memory to continue to drop over time. Low/decreasing free memory (in versions 5.0.0 and above) is NOT a sign of a memory consumption issue. Memory is being reassigned as needed in these newer versions of software updates.
- Refer to knowledge base article on our site: <http://support.spectracomcorp.com/articles/FAQ/free-cpu->

[memory?q=free%20mem&](#)

- top automatically updates once every 5 seconds by default.
- Refer to Mantis case 3029.
- CPU usage is a comparison of processor “use time” versus “rest time”.
- CPU usage is high in the SecureSync because ETX is a single core processor running multiple threads.
 - In version 5.2.0, CPU usage is running around 85 to 90%. After downgrade to version 5.1.2, similar values still being reported (around 91%).
 - Though the usage is high, NTP is the one of the higher priority threads. So NTP performance is NOT affected in any way by the high CPU usage.

C) Free, free mem, free -m commands

- The free memory commands report the same values as the response to the “top” cli command (towards the top of the response).
 - Refer also to the “top” command description further above.

free / free mem vs free -m (free -m reports in Megabytes instead of kilobytes)

```
lspadmin@spectracom ~1$ free
lspadmin@spectracom ~1$ free
Mem:          total        used          free      shared    buffers    cached
-/+ buffers/cache: 38132      469516
Swap:          0              0              0
lspadmin@spectracom ~1$ free mem
lspadmin@spectracom ~1$ free mem
Mem:          total        used          free      shared    buffers    cached
-/+ buffers/cache: 38132      469516
Swap:          0              0              0
lspadmin@spectracom ~1$
```

free -m (reports in Megabytes instead of kilobytes)

(With version 5.?.0 installed)

```
l4 root      20  0  0  0  0 S  0.0  0.0  0:00.00 kcompactd0
spadmin@spectracom ~ $ free -m
Mem:          total        used          free      shared  buff/cache  available
Swap:          0              0              0
```

(With version 5.0.2 installed)

```
spadmin@spectracom ~ $ free -m
Mem:          total        used          free      shared    buffers    cached
-/+ buffers/cache: 42      452
Swap:          0              0              0
```

(With version 4.8.8 installed)

```
Spectracom NetClock 9483 Version 5.0.0
spadmin@spectracom ~ $ free -m
Mem:          total        used          free      shared    buffers    cached
-/+ buffers/cache: 62      431
Swap:          0              0              0
```

D) cat /proc/meminfo

- /proc/meminfo also reports info on free memory

```
spadmin@Spectracom ~ $ cd /proc
spadmin@Spectracom /proc $ cat meminfo
MemTotal:        305984 kB
MemFree:         360672 kB
MemAvailable:    425388 kB
Buffers:         21444 kB
Cached:          63236 kB
SwapCached:      0 kB
Active:          106986 kB
Inactive:        22236 kB
Active(anon):    54692 kB
Inactive(anon):  4316 kB
Active(file):    52264 kB
Inactive(file):  17920 kB
Unevictable:     5012 kB
Mlocked:         5012 kB
SwapTotal:       0 kB
SwapFree:        0 kB
Dirty:           28 kB
Writeback:       0 kB
AnonPages:       48824 kB
Mapped:          34568 kB
Shmem:           11012 kB
Slab:            6720 kB
SReclaimable:    3256 kB
SUnreclaim:     3464 kB
KernelStack:    672 kB
PageTables:     1076 kB
NFS_Unstable:    0 kB
Bounce:         0 kB
WritebackTmp:   0 kB
CommitLimit:    252972 kB
Committed_AS:   251432 kB
VmallocTotal:   524168 kB
VmallocUsed:     9160 kB
VmallocChunk:   515796 kB
DirectMap4k:    12032 kB
DirectMap4M:    503808 kB
spadmin@Spectracom /proc $ ^C
```

E) Linux **vmstat** and **vmstat 1** CLI commands

- Refer to sites such as: http://linuxcommand.org/man_pages/vmstat8.html

Vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length *delay*. The process and memory reports are instantaneous in either case. **vmstat** (one time) and **vmstat 1** (continuous output)

```
spadmin@Spectracom111 ~ $ vmstat
procs  -----memory-----  ---swap--  -----io-----  -system--  -----cpu-----
 r  b  swpd  free  buff  cache  si  so  bi  bo  in  cs  us  sy  id  wa  st
 1  0    0 326564 21692 81696  0  0  1  13  297  256  57  34  10  0  0
spadmin@Spectracom111 ~ $
```

Field descriptions for the **vmstat** command

Memory

swpd: the amount of virtual memory used.

free: the amount of idle memory.

buff: the amount of memory used as buffers.

cache: the amount of memory used as cache.

inact: the amount of inactive memory. (-a option)

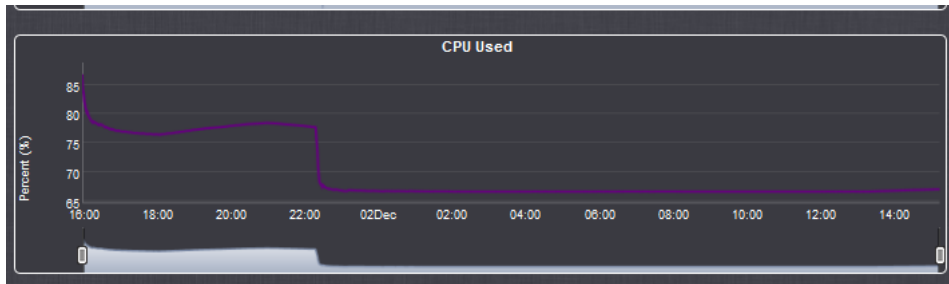
active: the amount of active memory. (-a option)

Reading the CPU usage (ETX module - “outer CPU”)

- CPU usage can be read/viewed via various methods, including a graph in the newer web browser (starting in v5.3.1), via CLI commands or via SNMP.

1. “CPU Used” graph towards the bottom of the Tools -> System Monitor page of the newer browser

- This graph available starting in update version 5.3.1



Details of this graph

Partial email from Tim Hammer (24 Sept 2021) CPU Used is determined using data obtained from the Linux kernel and represents the percentage of time that the CPU is busy working (vs. being idle). Similar to memory usage, normal operations will result in fluctuations as applications and the kernel provide the unit's functionality.

2. Reading the “outer” processor’s CPU usage stats via CLI (telnet/SSH or serial)

- Can use CLI commands such as “top”, “free”, `free -m` or `vmstat` to read the CPU's free memory.

A) **top** command via CLI to retrieve the CPU memory usage is a standard linux command

Refer to: http://linux.about.com/od/commands//blcmd1_top.htm

```
top - 15:08:48 up 16:50, 1 user, load average: 1.56, 1.43, 1.61
Tasks: 73 total, 1 running, 72 sleeping, 0 stopped, 0 zombie
Cpu(s): 24.4 us, 18.2 sy, 0.0 ni, 57.4 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 505944 total, 138364 used, 367580 free, 21432 buffers
KiB Swap: 0 total, 0 used, 0 free, 62908 cached Mem
```

%CPU: The task's share of the CPU time since the last screen update, expressed as a percentage of total CPU time per processor.

“CPU” associated fields

us: Time spent running non-kernel code. (user time, including nice time)

sy: Time spent running kernel code. (system time)

id: Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time (**Note: CPU usage is the inverse of this value. So if the idle is 15, the usage is 85%**)

wa: Time spent waiting for IO. Prior to Linux 2.5.41, shown as zero.

- “**top**” CLI command to retrieve the CPU usage is a standard linux command.
- top automatically updates once every 5 seconds by default.
- Refer to Mantis case 3029.
- CPU usage is a comparison of processor “use time” versus “rest time”.
- CPU usage is high in the SecureSync because ETX is a single core processor running multiple threads.
 - In version 5.2.0, CPU usage is running around 85 to 90%. After downgrade to version 5.1.2, similar values still being reported (around 91%).
 - Though the usage is high, NTP is the one of the higher priority threads. So NTP performance is NOT affected in any way by the high CPU usage.

A) Linux **vmstat** and **vmstat 1** CLI commands

- Refer to sites such as: http://linuxcommand.org/man_pages/vmstat8.html

Vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length *delay*. The process and memory reports are instantaneous in either case. **vmstat** (one time) and **vmstat 1** (continuous output)

```
spadmin@Spectracom111 ~ $ vmstat
procs -----memory----- ---swap-- -----io----- -system-- -----cpu-----
 r  b   swpd   free   buff   cache   si   so    bi   bo    in   cs  us  sy  id  wa  st
 1  0     0 326564 21692  81696    0    0    1   13   297  256  57  34  10  0  0
spadmin@Spectracom111 ~ $
```

Field descriptions for the **vmstat** command

CPU

These are percentages of total CPU time.

us: Time spent running non-kernel code. (user time, including nice time)

sy: Time spent running kernel code. (system time)

id: Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time.

wa: Time spent waiting for IO. Prior to Linux 2.5.41, shown as zero.

To calculate total CPU usage, **add us and sy**

B) Reading the “outer” processor stats Via SNMP

- Check this linux OIDs <http://www.debianadmin.com/linux-snmp-oids-for-cpumemory-and-disk-statistics.html> . These OIDs are common to SMNP for linux systems and are not Spectracom specific.

SNMP object for reading “outer” CPU usage for all Versions of SecureSync software: **.1.3.6.1.2.1.25.3.3.1.2**

```
spadmin@Spectracom111 ~ $ snmpwalk -t 5 -v 2c -c snmpptest 10.2.100.177 .1.3.6.1.2.1.25.3.3.1.2
HOST-RESOURCES-MIB::hrProcessorLoad.196608 = INTEGER: 86
```

Note: Software Versions 5.2.1 and above can also use the following OIDs

percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0

raw user cpu time: .1.3.6.1.4.1.2021.11.50.0

percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0

raw system cpu time: .1.3.6.1.4.1.2021.11.52.0

percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0

raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0

raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

Reports of high CPU usage (spikes in CPU usage or constant high CPU usage)

Factors potentially adversely affecting CPU usage

- Network vulnerability scanner
 - Refer to Salesforce Case 252952
 - Review Auth logs for entries of a device logging in.
 1. **Email from Ron Dries (24 Nov 2020)** I took a look at the logs on case 252952
 2. The auth.log shows the following user: infosec_scanner_corp_unix appearing to try to connect to the SecureSync repeatedly everyday around 00 – 01 UTC.
 3. My guess is they have a device on the network that is attempting to scan the SecureSync and this scanning process is most likely causing the CPU spikes.
- Having a more recent software version installed (**versions 5.8.0 and above**)

Per Dave Sohn (7 Sept 2018) CPU utilization increase is due to patches required for Spectre/Meltdown vulnerability fixes. Removing/protecting speculative execution by the CPU does have an effect on processing efficiency.
- Having an earlier, less-efficient software version installed (**such as versions 5.4.0 or below**)
- Having MANY NTP clients hitting the SecureSync at the same time (one or all interfaces)
- Timekeeper option enabled and running (i.e. Morgan Stanley)
- SNMP Manager(s) walking the SNMP MIB files (this can really increase usage)
- FTP (especially when navigating to different directories) or telnet,ssh and HTTP/HTTPS browser connections (especially when there are many simultaneous connections)
- Heavy network traffic

Recommended Suggestions

- 1) Obtain/review the log bundle (especially look at the sql database' ethernet data to see if high CPU usage correlates with heavy network traffic)
 - Version 5.4.0 added the **Tools-> Ethernet Monitor** page of the browser, to show Ethernet traffic graphs for Eth0. And the SQL lite database contains this same data for all the ethernet interfaces. Obtaining the log bundle allows the data in this database to be correlated to the CPU usage data. If both graphs increase at the same time, the usage was likely due to a spike in network traffic.
- 2) Confirm if customer is walking the SNMP MIBs from any SNMP Manager. If they are, have them temporarily stop this action and see what the usage drops to thereafter.
- 3) Find out how many computers/clients are syncing to the SecureSync via NTP. Keep in mind that the Management -> NTP Setup page includes NTP Throughput graphs of how often NTP is responding to NTP requests (can they send you these two graphs for review).
- 4) See how many computers are opening web browser or CLI connections at the same time.
- 5) Do they have the Model 1204-06 GB card installed? If so, how many of these three ports are connected to networks? Or is just eth0 only?

Email Keith sent to Morgan Stanley (15 Jul 16) I'll start by saying the logs show this unit appears to be operating normally, as reviewed by our engineers and me. I have a couple of questions for you, though.

The alert you received from the SNMP Manager indicates the CPU usage exceeded 85% “for more than the acceptable time period.”. What is the “acceptable time period” for the SNMP Manager? - Also, was this a one-time received usage alert, or are they periodically being sent from the SecureSync? if it was a one-time only alert, it may have been due to a period of heavier than normal network traffic. the logs capture the usage once-per-minute, at about 30 seconds into the minute. I didn't observe any spikes, but momentary spikes, which occur as part of normal operation may not get logged.

Many different conditions can affect the normal and periodic spikes in CPU usage valued, including SNMP operations (walking the SNMP MIBS has a large impact on this value) and heavy network traffic, for examples. For this reason, we recommend not

walking the SNMP MIBS – we recommend polling individual values instead of walking the mib files. Is your SNMP Manager(s) walking the SecureSyncs' MIB files? If so, how often are the MIBs being walked (periodically or continuously)?

SSH and other logins can also increase the CPU usage above its typical values. The typical "idle" CPU usage is around 60% to 70%. But SNMP Walks and other external connections can cause this to increase to around 90% to 95%. To prevent the normal operation of the SecureSync from causing superfluous high CPU usage alerts being sent, I recommend setting the alert threshold for CPU usage of the SecureSync in your SNMP Manager to a value such as 95% for instance (note that high CPU usage does not adversely affect the timing capabilities of the unit),

If the alerts are continuing to be sent (it wasn't just a one-time occurrence), find out if the SNMP Manager is walking the MIB files and was there one or more users logged into the SecureSync when the alert was sent? If the Manager is walking the MIB files, we recommend stopping the walks and then see if the alerts stop being sent.

Partial Draft email Keith sent (20 Sept 2018) for a customer concerned about high cpu usage.

My response

To begin, and though its CPU usage is not a concern for the SecureSync's operation itself (it's merely a "perception" condition for users), the version of software installed each SecureSync is a direct factor towards its typical CPU usage (as are other factors as well, such as the Number of NTP clients polling each SecureSync for its time at any given moment, how busy are the networks the SecureSync is connected to, the number of users simultaneous users logged into its web browser/CLI interface, the number of active SNMP connections/walking the SNMP MIBS, etc).

Before adjusting your CPU usage alert threshold levels accordingly for remotely monitoring the SecureSync, which version of software is currently installed in at least SecureSync NTPPTN32? And what is its typical CPU usage (note the CPU usage can be near, or at, 100% without adversely affecting the SecureSync's operation).

Note: If you aren't sure what version of software is currently installed (and if the unit is accessible):

- With the newer black background web browser (starting in software version 5.1.0), the System version is reported in the **Tools -> Upgrade/backup** page of the browser.
- With a CLI command prompt (telnet, ssh or front panel RS-232 connection) type **version** <enter>. The response indicates the current version.
- With earlier versions (which the web browser has a white/gray background) the Archive software version is reported at the top of the **Tools -> Versions** page.

Software version factors which can affect typical CPU usage observed:

- **Software Version 5.8.0 and above being installed:** CPU utilization increase in newer versions of software is due to patches required for Spectre/Meltdown vulnerability fixes. Removing/protecting speculative execution by the CPU does have an adverse effect on processing efficiency.
- **Earlier software versions, such as versions 5.4.0 and 5.3.1 being installed:** Software version 5.4.1 increased the efficiency of the software, thus allowing for a small decrease in the CPU usage typically observed,

Other Questions / suggestions for you:

- 1) Are you walking the SecureSync's SNMP MIB files from one or more SNMP Managers? If you are, try temporarily stopping this action and see what its usage drops to thereafter (walking its MIB files, instead of using SNMP Gets for particular object values, can significantly increase its CPU usage).
- 2) The **Management -> NTP Setup** page of the web browser includes "**NTP Throughput graphs**" of how often NTP in the SecureSync is responding to NTP requests (can you send us a screenshot of these two graphs for review)?
- 3) The SecureSync's log bundle records ethernet data, which we can use to see if periods of higher CPU usage correlate with higher network traffic. Further below is info on how to upload to us the unit's logs and configs bundles (two separate files), if you would like us to review these files for you, to see what they indicate.
- 4) Does the SecureSync have the Model 1204-06 GB Ethernet Option Card installed (adding three additional ethernet interfaces to the single ethernet interface, eth0, installed in all SecureSyncs)? If it does. how many of these three additional interface ports are connected to networks (just one, two of the three, or all three)? Or, is just the interface eth0 on the base chassis of all SecureSyncs (near the AC power connector) connected to a network?
- 5) How many computers are opening web browser or CLI connections to the SecureSync at the same time?
- 6) About how many computers/NTP clients are configured syncing to the SecureSync (tens of clients. or thousands of clients. for instance)? If you aren't sure how many clients/which clients are getting time from the SecureSync, this info can be obtained from a wireshark/tcpdump packet capture of UDP port 123 (the NTP port) on all ethernet interfaces of

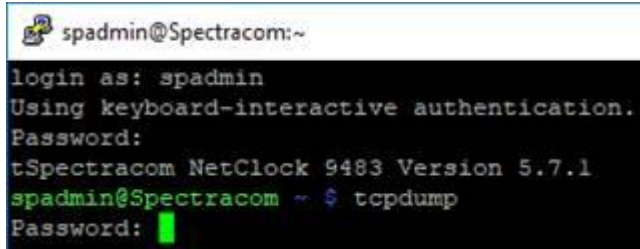
the SecureSync. Filter the capture using the “destination” address of the SecureSync (all NTP packets being sent to all SecureSync interfaces, eth0 thru eth3 which are connected to networks)

- A) **Just interface eth0 connected to a network**, type: **tcpdump dst port 123<enter>**
- B) **Specify which interfaces are connected to a network**, type **tcpdump dst port 123 -i** (lower case letter, like in “india”) **eth0 -i eth1 -i eth2 -eth3<enter>** (type only the ethernet interfaces which are connected to a network)

Example for only interfaces eth1 and eth3 connected to network type: **tcpdump dst port 123 -i eth1 -i eth3<enter>**

Notes about TCPdump:

- 1) use **CTRL + C** to stop a capture in progress
- 2) If the tcpdump command responds with a password (as shown below) tcpdump has been disabled in the time sever (and can't be re-enabled without performing a full upgrade/restore to factory default):



```
spadmin@Spectracom:~  
login as: spadmin  
Using keyboard-interactive authentication.  
Password:  
tSpectracom NetClock 9483 Version 5.7.1  
spadmin@Spectracom ~ $ tcpdump  
Password: █
```

Downloading and sending us the log bundle (include here the standard draft info on sending log/configs bundles)

False alerts due to NMS/NNMi being enabled in the SNMP manager

- Refer to (in this same doc) “False alerts due to NMS/NNMi being enabled in the SNMP manager” for details

SecureSync's Gentoo Operating System (OS) - Software licenses/licensing

A) Operating System (Linux distribution)

➤ SecureSync runs on a Linux OS.

1. Much earlier versions (prior to 5.0.1??) were Brutal Linux

Internal Note (don't advertise this to customers) our Linux OS (Brutal Linux) isn't a standard distribution (such as Red Hat or CentOS for examples). It was originally pieced together from different available source code. If a customer asks which distribution we were using, it was a **PROPRIETARY** version of **linux**.

2. Much more recent versions (5.0.1 and below, I believe) are gentoo linux

Base Gentoo package versions

➤ Refer to Merged Salesforce Cases 278570/278650

Checking current base Gentoo Version via SSH (also reported in Tenable ACAS scan)

"I can confirm the OS version by logging into the unit over SSH and running the command **cat /etc/gentoo-release**. It returns the same output as the ACAS scan."

- SecureSync Version 5.9.4 has **gentoo version 2.6** installed.
 - JIRA ticket SSS-1243 (Jan 2022) request to update gentoo to 4 or higher

B) Linux Kernel versions

For Kernel versions installed in the various software versions – Refer to the software updates spreadsheet: [I:\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates\Software release dates.xlsx](#)

- The Linux kernel in software update version 5.9.4 is **4.14.228**
- The kernel version for Archive software versions 4.8.6, 4.8.7, 4.8.8 and 4.8.9 is version **2.6.15**.

• CLI command to read Linux OS (kernel) version and distribution version: **cat /proc/version**

```
spadmin@Spectracom ~ $ cat /proc/version
Linux version 3.8.13-gentoo (root@localhost) (gcc version 4.6.3 (Gentoo 4.6.3 p1
.13, pie-0.5.2) ) #1 PREEMPT Wed Jul 3 05:07:14 Local time zone must be set--see
2
```

➤ Archive software version 5.0.0 updated the kernel version to version 3.8.13.

- **Internal Note (don't advertise this to customers)** If a customer asks which distribution we are using, it is **Gentoo** linux (But don't volunteer this information if just indicating "Linux OS" is enough info for them.

Software licenses of open source software

➤ Refer to Section 12 of the SecureSync manual for information on licensing for the software modules used in SecureSync (including the following):

- 2) NTP
- 3) OpenSSH
- 4) OpenSSL

Ability to view open source software licenses in the browser.

- Use the Browser's "Developer Tools" (shortcut: CTRL + Shift and the letter "I", and select "debugger") to view the Javascript files.
- For example, MIT license (for code such as dygraph) just requires a header be added to our code.

MIT's dygraph license for graphs.

- Refer to steps above to view the dygraph.js file (Select "dygraph-combined.js") and the license is shown in the top line.

kernel traceback

- Refer to Salesforce case 14369
- Indication of an issue occurring

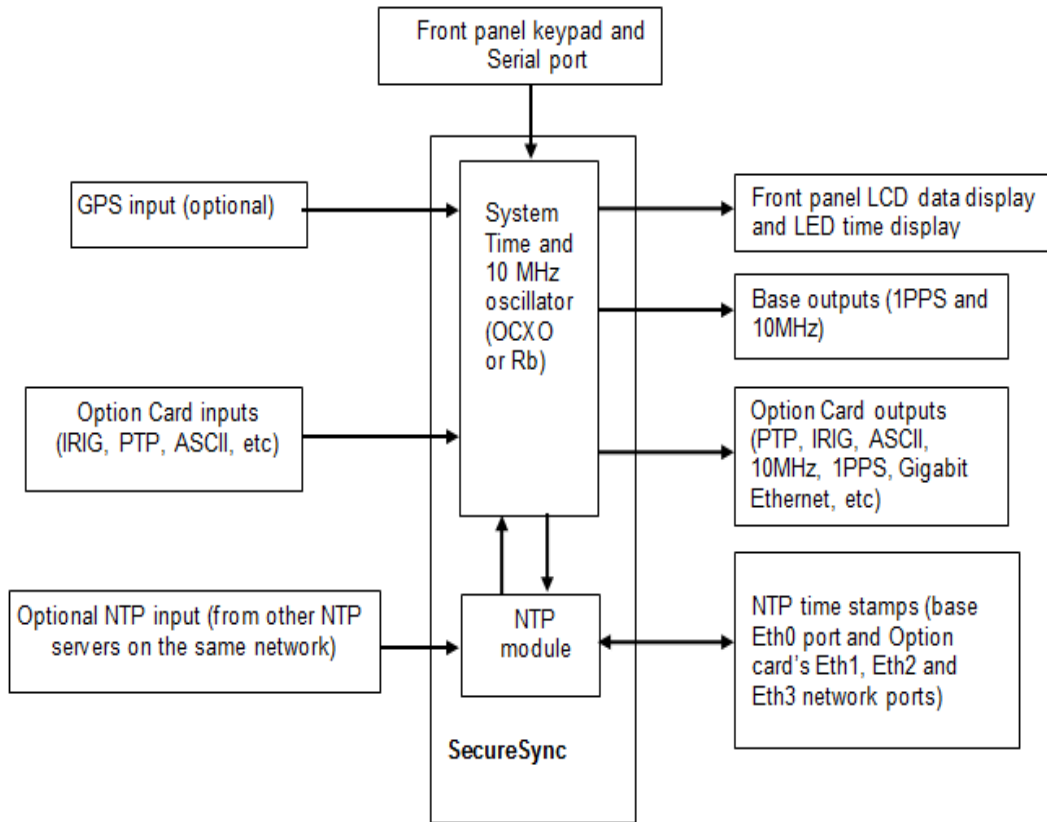
Email from Chris Johnston with PDT Partners We had a brand new unit come to us that was having some issues, we went to go and reboot the device (via command line) and were unable to do so. Rob did some debugging and noticed we saw a kernel traceback which I pasted below and a bunch of processes in the D state. We ended up having to manually reboot the device. How do you want to us to get items like this up to support so we don't have to bug you for the small stuff?

```
> [118944.087216] BUG: unable to handle kernel NULL pointer dereference at
> (null)
> [118944.087540] IP: [<c115d0d5>] __rb_insert_augmented+0x25/0x150
> [118944.087787] *pde = 00000000 [118944.087879] Oops: 0000 [#1] PREEMPT
> [118944.088012] Modules linked in: e1000e(O) e100 8139too tsyncpci(O)
> pps_core
> [118944.088022] Pid: 2314, comm: khtd Tainted: G      O 3.8.13-gentoo #1
> /AMD-GX3
> [118944.088022] EIP: 0060:[<c115d0d5>] EFLAGS: 00210246 CPU: 0
> [118944.088022] EIP is at __rb_insert_augmented+0x25/0x150
> [118944.088022] EAX: 00000000 EBX: dcc5fab8 ECX: dcc5fed8 EDX: dcd564e4
> [118944.088022] ESI: dcc5f3c8 EDI: c108d550 EBP: dcc99ecc ESP: dcc99eb8
> [118944.088022] DS: 007b ES: 007b FS: 0000 GS: 0033 SS: 0068
> [118944.088022] CR0: 8005003b CR2: 00000000 CR3: 1cc54000 CR4: 00000090
> [118944.088022] DR0: 00000000 DR1: 00000000 DR2: 00000000 DR3: 00000000
> [118944.088022] DR6: ffff0ff0 DR7: 00000400
> [118944.088022] Process khtd (pid: 2314, ti=dcc98000 task=dcc8d040
> task.ti=dcc98000)
> [118944.088022] Stack:
> [118944.088022] dcd564e4 dcdab9a0 dcc5f3d8 dcc5f3c8 dcd564e0 dcc99ee4
> c108ddd8 dcc4c580
> [118944.088022] dcc5f3c8 dcc4c5d8 dcc5f420 dcc99f24 c1027ed3 dcc5fed8
> dcd56518 def396f8
> [118944.088022] dcc5fed8 dcc5fedc dcc5fed0 dcc5fec8 def396c0 00000001
> dcd564e0 dcc4c580
> [118944.088022] Call Trace:
> [118944.088022] [<c108ddd8>] __vma_link_rb+0x5b/0x70
> [118944.088022] [<c1027ed3>] dup_mm+0x213/0x3e0
> [118944.088022] [<c10288e0>] copy_process+0x810/0xe10
> [118944.088022] [<c1028f87>] do_fork+0x87/0x220
> [118944.088022] [<c10291db>] sys_clone+0x2b/0x40
> [118944.088022] [<c1331f7e>] sysenter_do_call+0x12/0x26
> [118944.088022] Code: b4 26 00 00 00 00 55 89 e5 57 89 cf 56 53 83 ec 08 8b
> 08 89 55 ec 85 c9 0f 84 f2 00 00 00 8b 19 f6 c3 01 75 51 8b 53 04 89 de 39
> <d1> 74 50 85 d2 74 05 f6 02 01 74 57 8b 71 04 39 c6 0f 84 94 00
> [118944.088022] EIP: [<c115d0d5>] __rb_insert_augmented+0x25/0x150 SS:ESP
> 0068:dcc99eb8
> [118944.088022] CR2: 0000000000000000
> [118944.108571] ---[ end trace 64832b828d2e0419 ]---
```

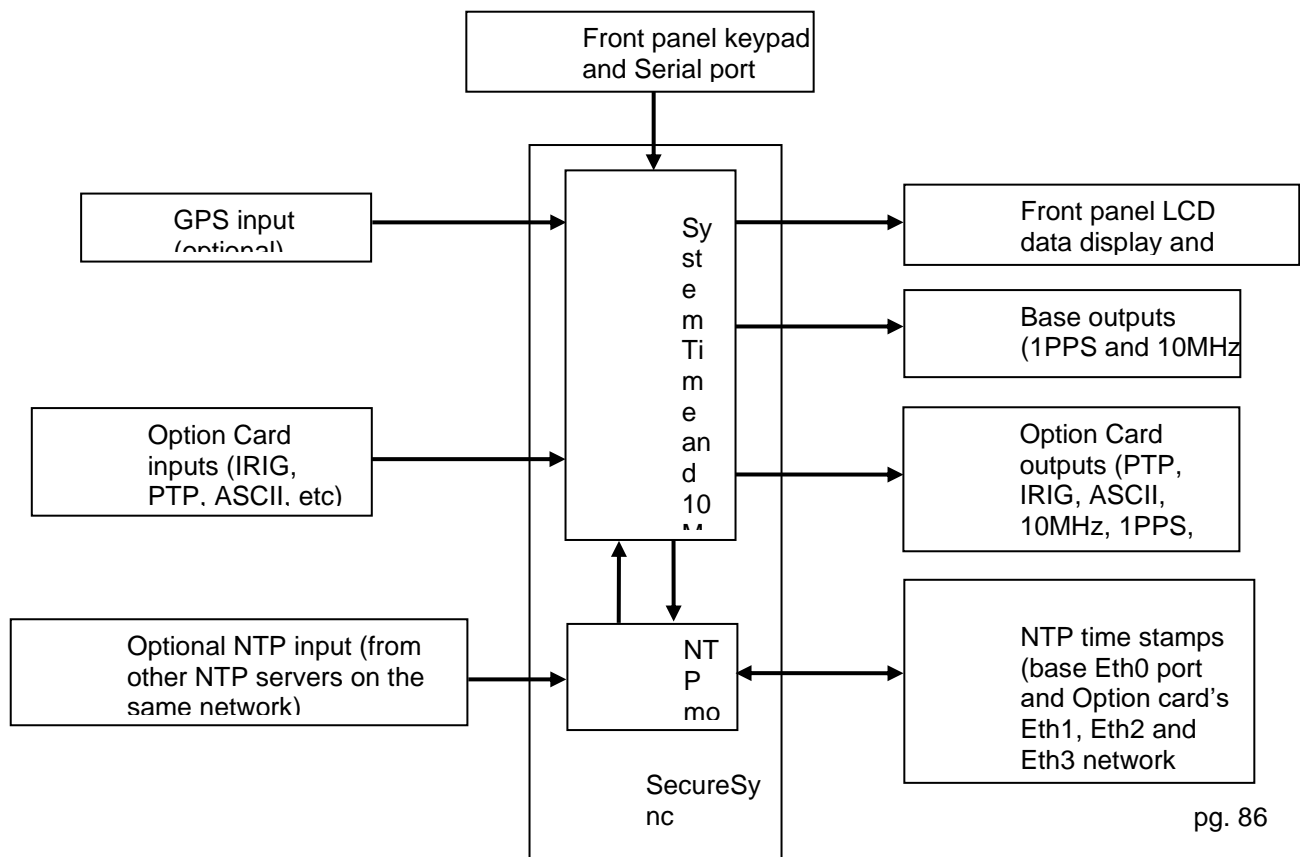
Q-Keith Asked Dave Sohn: Is this just debug software they are referring to? Or a potential issue with the unit?

A-Reply from Dave Sohn The kernel traceback means that some running software had a serious issue. Having a bunch of processes in the “D” state would also be indicative of software running into issues. It could be a potential issue with the unit. I haven't seen this, and looking at a running system in engineering I don't see processes in the “D” state.

System operation block diagram (for internal use only)



(for edits)



CAD/3D drawings

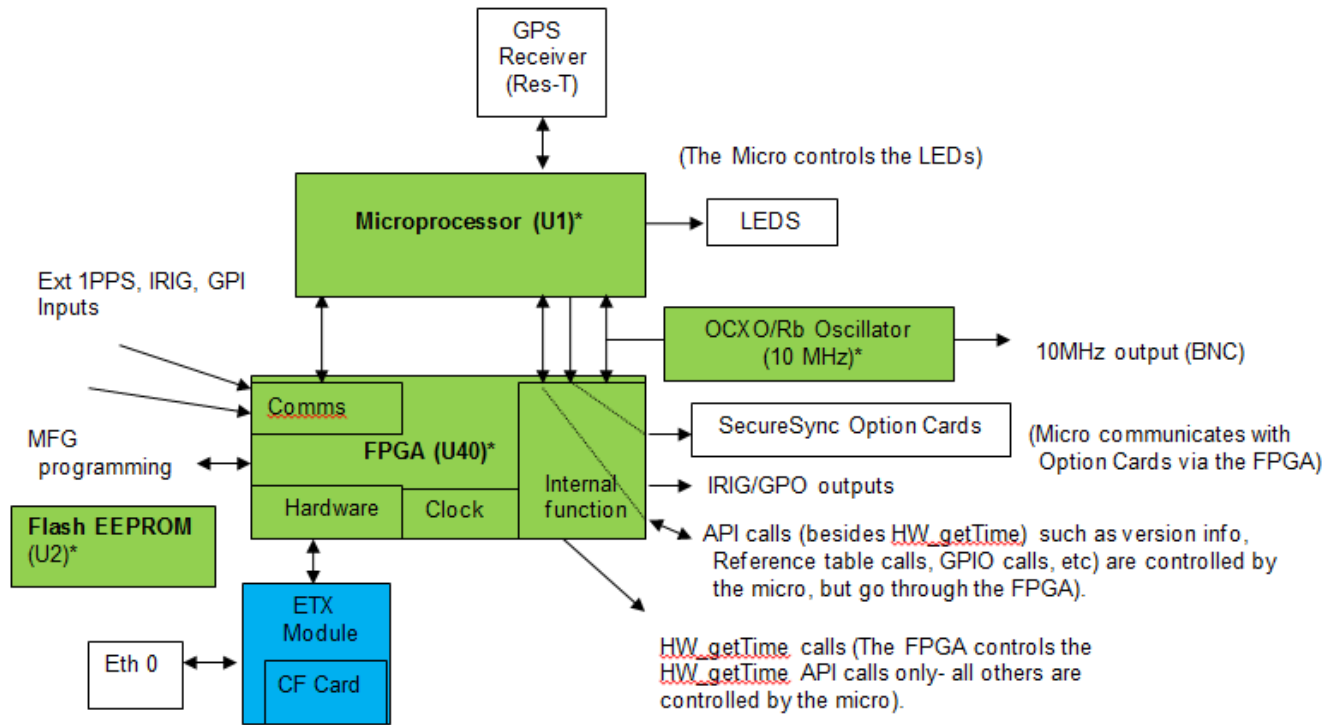
➤ Refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CAD - 3D drawings](#)

Hardware block diagram

Note: for internal use only

* denotes item is part of the Kramden Timing System (KTS) (Green fill items)

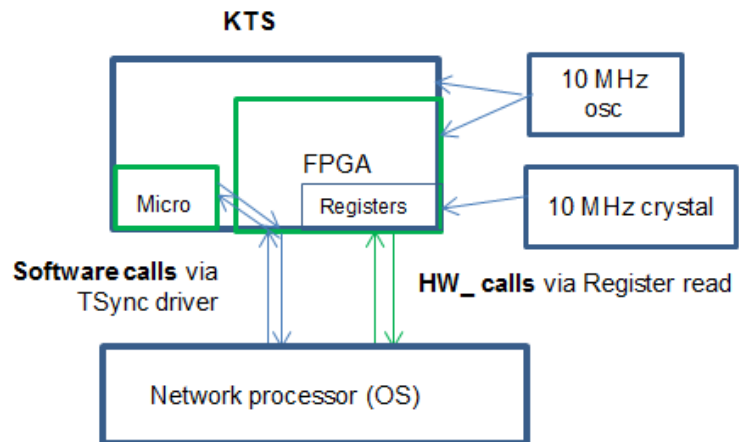
Network processor software (blue fill)



* denotes item is part of the Kramden Timing System (KTS) (in green)

Kramden Timing System (KTS)

Function: “Brains” of system timing, input reference functionality , all of the TSync related calls (GetTime calls, oscillator control, GPIO, GPS)



4.2 Kramden Digital Timing Core

The Kramden timing core is a combination of hardware and firmware that implements an autonomous, but configurable timing system. The Kramden timing core keeps time in hardware inside of an FPGA and manages the time with firmware running on a Freescale Coldfire embedded processor that has 512 Kbytes of internal flash and 64 Kbytes of internal SRAM, along with many embedded peripheral devices. The Kramden digital core has 8 Mbytes of external flash and 8 Mbytes of external SDRAM memory. For thorough descriptions of the Kramden timing core hardware, refer to the KTS-202 Kramden FPGA Requirements document and the KTS-200C Kramden Hardware design disclosure document called out as reference items. A block diagram of the Kramden digital core modified for use in Lafayette is shown below. A brief overview of the Kramden Timing core follows.

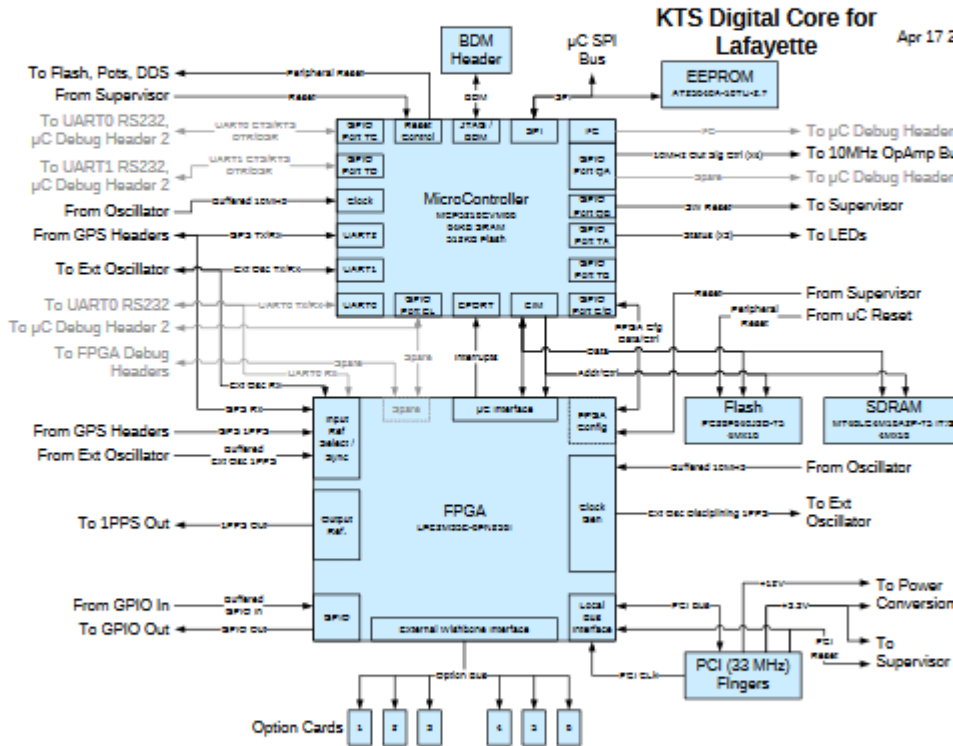


Figure 3 – Kramden Timing Core block diagram

KTS consists of the following four components:

A) Microprocessor (U1):

- The Micro controls all API calls (besides HW_GetTime) such as version info, Reference table calls, GPIO calls, etc), but these go through the FPGA (not directly to/from the micro).
- The Micro controls the GPS receiver operation. The “GR_” API calls for the GPS receiver go through the FPGA to the micro.

B) FPGA (U40):

- The FPGA handles the communications with the Microprocessor.
- The FPGA itself handles and responds to the HW_GetTime API calls (all other API calls are handled by the micro, even though they go through the FPGA).

C) EEPROM (U2):

- Flash memory
- The EEPROM programs and stores info for the FPGA.

D) 10 MHz oscillator

Notes:

- 1) The EEPROM is reprogrammed during the firmware update process.
- 2) A programming issue with the EEPROM will prevent the micro from working.
- 3) A problem with only the micro allows HW_GetTime API calls to still work, but no other API calls will work (try several different API calls to verify micro issue).
- 4) A problem with the FPGA will allow GPS operation to be normal (can still sync and the LEDs will operate normally) but the user won't be able to communicate with the GPS receiver, for instance, because API calls can't get through.
- 5) If the FPGA is not operating, even if the micro is still running, there will be no communication with the micro, so the micro will appear to not be running. However, with the micro still running, the LEDs will still work.

**Indications of KTS not running

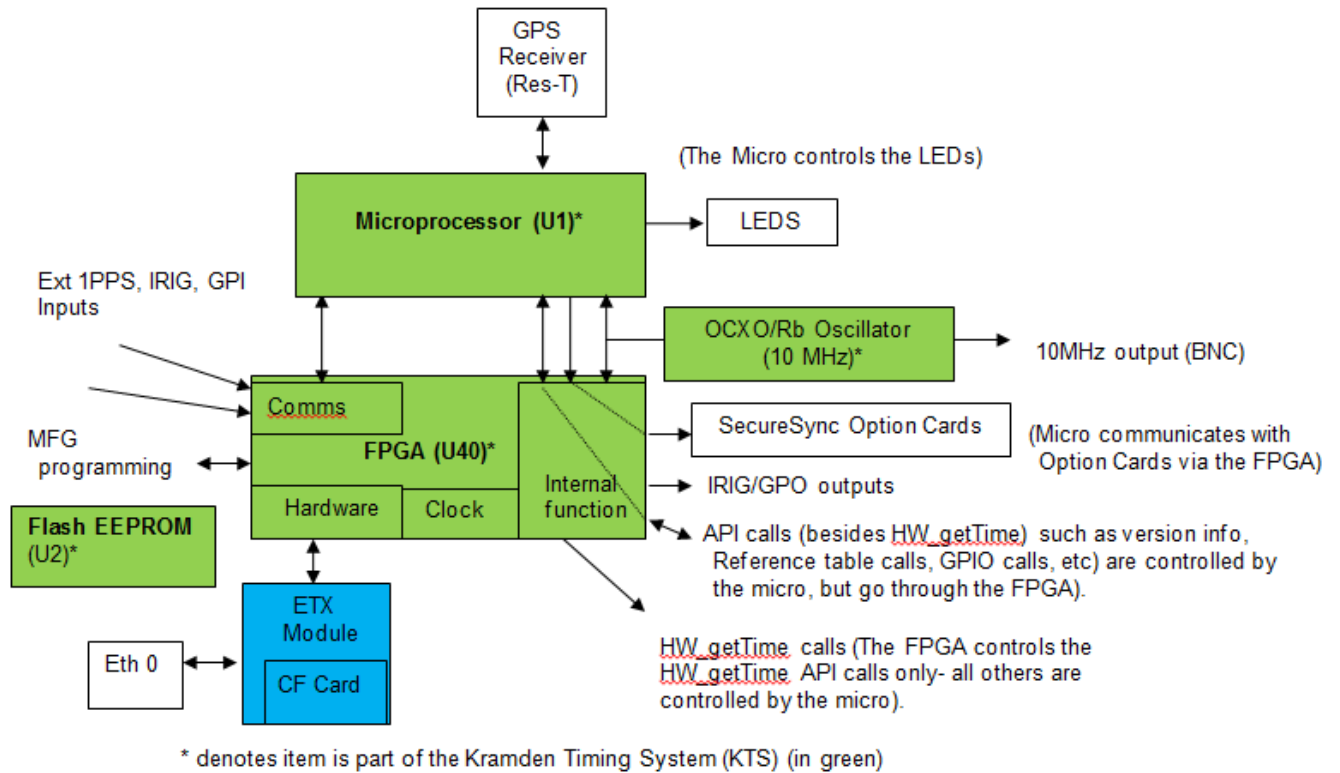
- Front panel LED time display frozen (not incrementing)
- Potentially- Several "KTS failed to read" log entries in the logs
- Potentially- difficulty with communicating with the browser/CLI due to ETX not being able to talk to KTS.

**ktsif.conf and ofdf.conf files

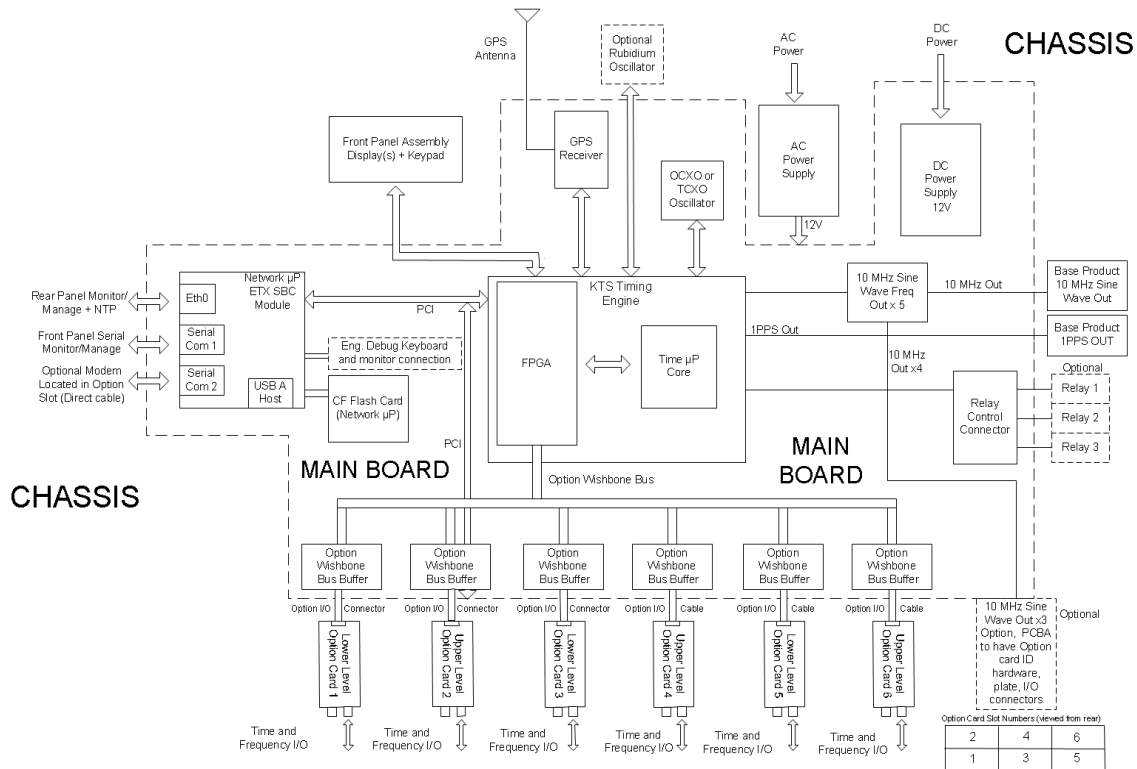
- Refer to: <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>

Network Processor software (NPS) (main software versions)

- The two Blue-fill items in the diagram below (the ETX module and the CF card)



- Controls: web browser, CLI interfaces (ssh, telnet, etc), NTP and other daemons, LDAP/Radius, LEDs
- Consists of the following two components:
 - **ETX module**
 - **CF Card (where the Linux OS software resides)**



Halt/Halt-Shutdown performed

- When either a Halt or Halt/Shutdown is performed, the Network Processor Software (NPS) stops running. However, the KTS Timing system continues to operate.

SecureSync Ancillary kits, (Anc kits/rack ears/brackets, manual CD, etc)

List of SecureSync Anc Kits (as of at least May 2022):

ITEM NUMBER	ITEM NAME
1200-0000-0701 rev 3	ANC KIT, SECURESYNC, N. AMERICA, AC ONLY
1200-0000-0702 rev 3	ANC KIT, SECURESYNC, N.AMER, AC & DC OPT
1200-0000-0703 rev 3	ANC KIT, SECURESYNC, DC ONLY
1200-0000-0704 rev 3	ANC KIT, SECURESYNC, RUGGED/NETAL KIT
1200-0000-0705 rev 2	ANC KIT, SECURESYNC, EURO, AC ONLY
1200-0000-0706 rev 2	ANC KIT, SECURESYNC, EURO, AC & DC OPTION
1200-0000-0707 rev 2	ANC KIT, SECURESYNC, UK/IRE, AC ONLY
1200-0000-0710 rev 3	ANC KIT, SECURESYNC, REAR BRACKET
1200-0000-0711 rev 2	ANC KIT, SECURESYNC, AC ONLY
1200-0000-0712 rev 2	ANC KIT, SECURESYNC, AC & DC OPT
1200-0000-0715 rev 4	ANC KIT, SECURESYNC 1000-ENHANCED UPM
1200-0000-0716 rev 2	ANC KIT, SECURESYNC HUGHES CGU CABLES
1200-0000-0717 rev 1	Ancillary Kit, Alarm Indicator

Hughes CGU SecureSync Anc Kit (1200-0000-0716) (as of at least May 2022)

#	ITEM NUMBER	ITEM NAME	CATEGORY
1	1200-1009-0801 rev 2	SECURESYNC HUGHES CGU ANC KIT LABEL	Label
2	CA01R-TNTN-0036 rev 1	CABLE ASSY,TNC MALE/TNC MALE, 36", DOUBLE SHIELDED RG58 COAX	Cable Assembly
3	CA05R-D910-0001 rev 4	CABLE ASSY, HUGHES CGU STATUS CABLE, 36"	Cable Assembly
4	MP02-0003-0002 rev 2	LABEL STOCK, 6 UP	Label
5	TM01R-0050-0001 rev 1	TERMINATION, SMA, MALE, 50 OHM, DC to 18000 MHz, 1.0 W	Electrical Hardware
6	TM03R-0050-0001 rev 1	TERMINATION, TNC, MALE, 50 OHM, DC - 11 GHz, 1.0 W	Electrical Hardware

Anc Kits/Timing Products CD shipped with L3Harris 1200 SecureSync orders

- Excerpt of items shipped with an L3Harris 1200 SecureSync order (SO 99184) which shipped April 2022

ATP	Product	Description	Fulfillment	Contract Item	
<input type="checkbox"/>	1200-H002-0601 - SecureSync H433,1...	SecureSync H433,14,00,1C,00,00,00	Internal		10
<input type="checkbox"/>	1200-0000-0703 - ANC KIT, SECURES...	ANC KIT, SECURESYNC, DC ONLY	Internal		10
<input type="checkbox"/>	1200-0000-0710 - ANC KIT, SECURES...	ANC KIT, SECURESYNC, REAR BRACKET	Internal		10
<input type="checkbox"/>	1200-5003-6H01 - CD, "Timing Produc...	CD, "Timing Product Manuals", Harris Edi	Internal		10
<input type="checkbox"/>	1200-5000-H051 - QuickStart Guide, H...	QuickStart Guide, Harris SecureSync	Internal		10

Manual CDs

- CDs are no longer provided with SecureSyncs (as of Jan 2020)
 - See apparent exception for L3Harris (directly above). They apparently still receive the Timing Product Manuals CD, P/N 1200-5003-6H01 (as of at least May 2022)
- Refer to **ECO-2267** (in Arena, "Changes" tab): https://app.bom.com/changes/detail-affected?change_id=2397636348

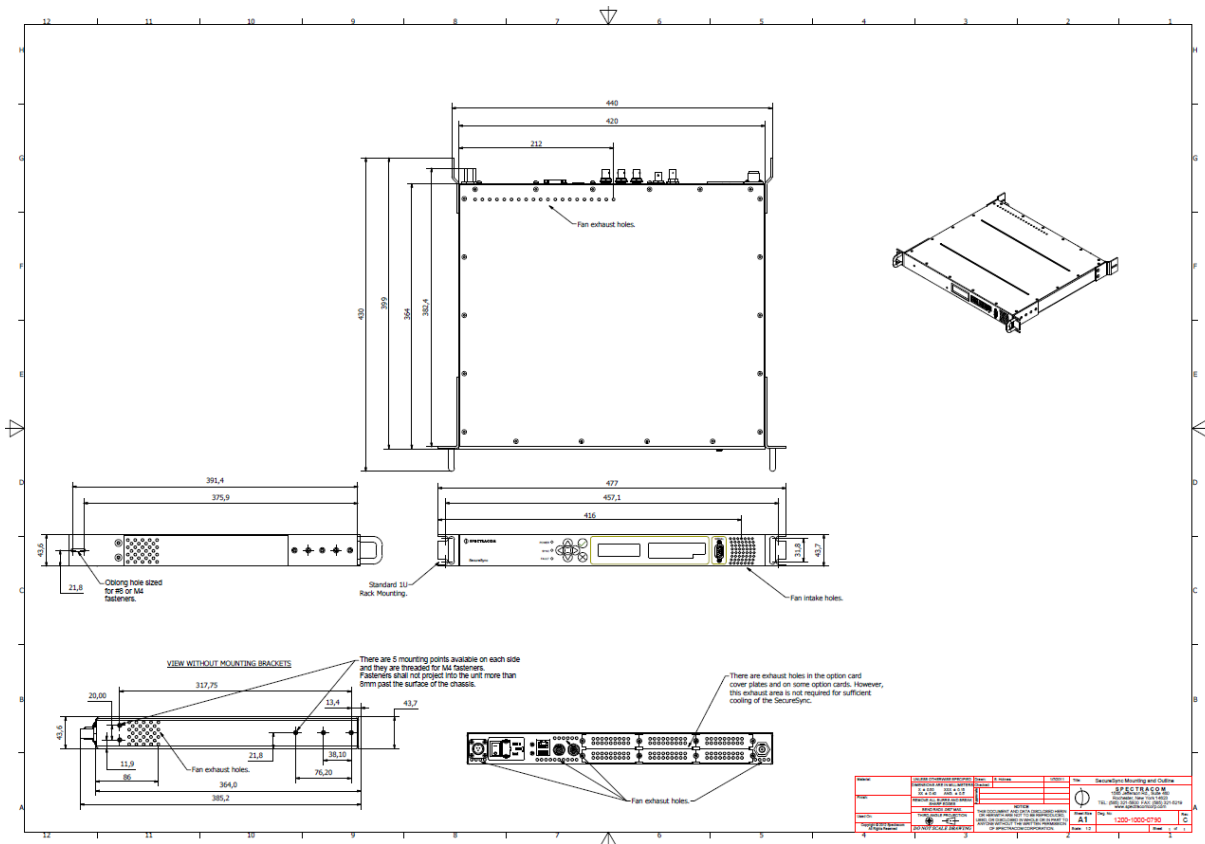
Rack-mounting brackets/rack ears/handles/Chassis material

Rack Mounting info in the online SecureSync user guide:

- http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/Mounting.htm?Highlight=bracket

Mounting hardware

- Drawing below (1200-1000-0790rd) at [I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\CAD - 3D drawings\SecureSync with Trimble or No GPS receiver\1200-1000-0790rd \(mtg and outline\).pdf](I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\CAD - 3D drawings\SecureSync with Trimble or No GPS receiver\1200-1000-0790rd (mtg and outline).pdf)



Rack mounting requirements:

- Refer to online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/Mounting.htm
 - The maximum ambient operating temperature must be observed. See [Mechanical and Environmental Specifications](#) for the operating temperature range specified for the type of oscillator installed in your SecureSync unit.
 - If the SecureSync unit is to be installed in a closed rack, or a rack with large amounts of other equipment, a rack cooling fan or fans should be part of the rack mount installation.
 - Installation of the unit in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

FAQs about chassis material and mounting

Email from Scott Holmes (6/1/11) The chassis and cover are both plated with a "conversion coating" called and are electrically conductive. The only parts on SecureSync that are different are the front panel plate with the overlay, which is anodized (corrosion resistance coated), and the rack ears (painted steel).

Q. What type of plating/conformal coating is used on the part?

A. No conformal Coating. Rohs Compliant Clear Iridite and Black Anodize.

Email from Scott Holmes (1/11/12)

We specify Cardinal C241-BK01 or equivalent powder coat paint on our products that are painted black.

Note: Responses to questions below in red are from Scott Holmes (3 Dec 2015)

Q What is the material of the unit chassis? **Material is 5052-H32 aluminum alloy**

Q What is the material of the front panel? Material is 5052-H32 aluminum alloy and the overlay is polycarbonate

Q What is the material of the mounting brackets? **12 Ga Cold Rolled Steel (1018)**

Q What are the dimensions, including thickness, of the mounting brackets? **12 Ga or 7/64 (.109) Thick. See attached drawing**

- Refer to drawing “**1165-1000-0714**” (in Arena) at: https://app.bom.com/items/detail-sourcing?item_id=1202841946&version_id=10221223518&orb_msg_single_search_p=1&redirect_seqno=8126093994

Q What type of fasteners are used to attach the mounting brackets to the body of the unit (chassis)? **Size M4 screws. Material is 18-8 Stainless Steel**

Q If included, what type of fasteners are used to attach the brackets to the equipment rack? **Not Included.**

Q Do you have mechanical CAD models of these units available (STEP or shrink-wrap) ? **See attached**

- Refer to “SecureSync M and 0_2.stp” at: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\CAD - 3D drawings>

M4 x 0.7 mm									
5	Fully Threaded	7.5	2.2	No. 2	70,000	DIN 965, ISO 7046-2	50	91698A423	7.92
6	Fully Threaded	7.5	2.2	No. 2	70,000	DIN 965, ISO 7046-2	50	91698A424	8.57
8	Fully Threaded	7.5	2.2	No. 2	70,000	DIN 965, ISO 7046-2	50	91698A426	6.29
10	Fully Threaded	7.5	2.2	No. 2	70,000	DIN 965, ISO 7046-2	50	91698A428	6.29

Product Detail

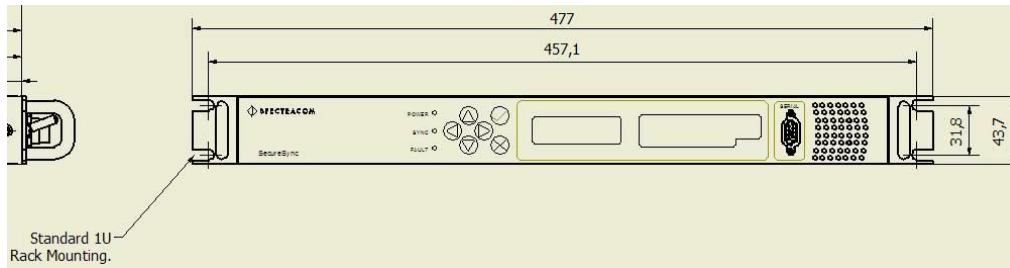
Black-Oxide 18-8 Stainless Steel Phillips Flat Head Screws, M4 x 0.7 mm Thread, 10 mm Long

Packs of 50

ADD TO ORDER

- o The thread size for these holes in the SecureSync chassis are **M4**
- o **M**: M4 screw (where the “M” stands for “metric”, and “4” is 4mm diameter)
- o 0.7mm thread
- o **18-8SS**: Made from 18-8 chrome/nickel stainless steel
- o **Length**= 10mm

Below is a current drawing that shows the rack ear slots for the Spectracom SecureSync mounting. Our Hardware design engineer also mentioned that the slot size of 7.1 +/- 0.3 is per specification EIA-310-D.



Stress testing/Type of material used for the rack ears

➤ Refer to Salesforce case 15341

Q What is the material of the mounting brackets?

A. Reply from Scott Homes (3 Dec 2015) 12 Ga Cold Rolled Steel (1018)

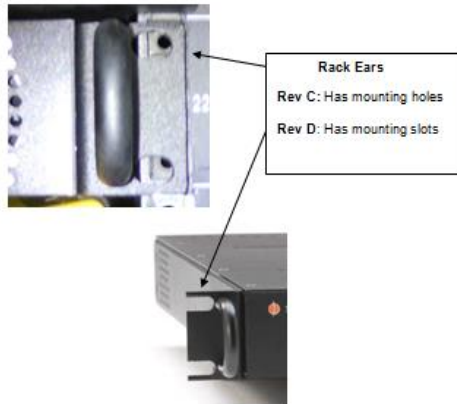
A Raytheon engineer is performing mechanical stress testing on a SecureSync and was asking about the mounting brackets. He wanted to know specifically what material these were made of.

Email from Dave Lorah to Sean Furey with Raytheon (12 Aug 2014) There is no specification for the exact type of alloy used in the manufacture of the Securesync Rack Mount brackets. The only specification is for 12 Ga. Cold rolled steel. We have these made for us by a local vendor.

Therefore the brackets could be made from any steel the manufacturer has on hand. So to be safe I would calculate based on the weakest or most common 12Ga cold rolled steel.

Rack ears are too short for 19 inch rack

- Refer to Case 6074 (Pavel May with Jane Street capital) for additional info
- Pavel reported the ears were too short, and sent us the following picture.



Note: The two rack ears are placed in a small static bag. The bag doesn't have a label on it indicating the P/N or Rev for the rack ears. The rev of the two ears is obtained by questioning if the ears have a mounting hole or mounting slots, as shown above.

(8/15/12) Scott Holmes responded to us with: They have the old 1165-1000-0714 Rev C rack ears. His rack is a bit out of tolerance or these ears would fit. We had one or two customers with this problem over the years so we submitted an ECN in November 2010 to open up the mounting holes in order to add more tolerance here. We now stock the Rev D part. If we send them a pair of the current 1165-1000-0714 Rev D rack ears, that will solve their problem

(8/13/12) Scott Holmes had also responded to us with: We have two APC racks in Engineering, one 19" and the other a 24" with 19" conversion kit. Both have SecureSync products mounted. Spectracom products that require rack mounting have been designed to meet Standard EIA-310-D for Cabinets, Racks, Panels and Associated Equipment.

The thread size for the rack ear holes are **M4** (the thread size for all of the other threaded holes in the chassis are **M3**).

Configuring/reconfiguring the power configuration

- Refer to the SecureSync Service Manual for full details on reconfiguring the input power configuration.
- Make sure the S/N tag and Registered Products in SAP both get updated accordingly.

Rack-mount slides (rackmount slides)

- Not currently available and not recommended (slides would block some of the cooling vents)

Q. I was hoping Spectracom has a recommended part number for 19" rackmount slides that can be used with the SecureSync line of products (Part Number 1200-XYZ).

A (10/25/12 reply from Keith, based on conversation with Scott Holmes) For your information, we don't currently offer any rack-mount slides for the Spectracom SecureSync. One potential concern of attaching rackmount slides to the sides of the chassis is that the slides would cover-up some of the cooling vents in the chassis. With several Option Cards installed in the SecureSync's Option Bays, the slides could potentially affect the cooling capabilities of the chassis. Because of the cooling vents, the SecureSync chassis is not currently designed to support the ability to add rails to the sides of the chassis

1200-1000-0704: Rugged Ancillary Kit (rear support brackets and AC power cord support)

- The available “Rugged Anc kit” consists of two rear support mounting brackets, brackets to secure the AC power cord in the SecureSync, and associated hardware

Email from Dave Sohn (16 Sept 2020) Below is the parts list for the 1200-1000-0704 Rugged Ancillary Kit for SecureSync

PART NO	QTY	DESCRIPTION
1200-1000-0706	2	Bracket, Rear
1200-1000-0707	1	Bracket, Cord
1200-1000-0708	1	Fork, Cord
HM11R-03R5-0004	2	Screw, PHP, M3-5, 18-8SS, 4mm, Thread Lock
HM20R-04R7-0010	4	Screw, FHP, M4, 18-8SS, 10mm, Black Oxide
HM72R-03R5-0002	1	Nut, Keps, M3 x 0.5mm, 18-8SS, 2.4mm HT

The **1200-1000-0706** are the rear brackets that are attached to the side, rear of the SecureSync units, using the (4) HM11R-04R7-0010 M4x10 screws.

The **1200-1000-0707**, **1200-1000-0708** are used to secure the AC power cord in the SecureSync using the two holes next to the power inlet module using (2) HM11R-03R5-0004 M3.5x4 screws and the HM72R-03R5-0002 nut.

1. Standard rear support brackets (A below) and Special rear support Brackets (B below)

- Each of the two Rear Brackets attach to the rear of the sides using two M4 screws for each bracket



A) TWO Standard rear brackets (1200-1000-0706) included in Rugged Anc kit (1200-0000-0704)

- **Summary:** Customers can purchase the two standard rear support brackets (1200-1000-0706) by purchasing the “SecureSync Anc Kit, Rugged Installation” (1200-0000-0704)
 - **Note from Dave S:** “The brackets we ship provide mounting features to support brackets that can be used depending on the depth of their racks. **They will still need to source the actual rear mounts.**”
 - **This anc kit (1200-0000-0704)** in Salesforce at: <https://orolia.my.salesforce.com/01tC0000004KorS?srPos=0&srKp=01t>
 - **This anc kit (1200-0000-0704)** in Arena at: https://app.bom.com/items/detail-spec?item_id=1203165694&version_id=10299429188&orb_msg_single_search_p=1

Email from Dave Sohn (16 Sept 2020) Below is the parts list for the 1200-1000-0704 Rugged Ancillary Kit for SecureSync

PART NO	QTY	DESCRIPTION
1200-1000-0706	2	Bracket, Rear
1200-1000-0707	1	Bracket, Cord
1200-1000-0708	1	Fork, Cord
HM11R-03R5-0004	2	Screw, PHP, M3-5, 18-8SS, 4mm, Thread Lock
HM20R-04R7-0010	4	Screw, FHP, M4, 18-8SS, 10mm, Black Oxide
HM72R-03R5-0002	1	Nut, Keps, M3 x 0.5mm, 18-8SS, 2.4mm HT

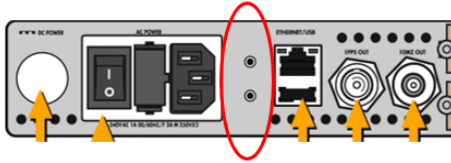
The **1200-1000-0706** are the rear brackets that are attached to the side, rear of the SecureSync units, using the (4) HM11R-04R7-0010 M4x10 screws.

More details for the info above:

- Our Part Number for the standard rear brackets themselves (and for the Mechanical drawing) is: **1200-1000-**

AC Power Cord support bracket (1200-1000-0707)

- AC Cord bracket attaches to two holes in the rear panel (near the AC power connector) using two M3.5 screws.

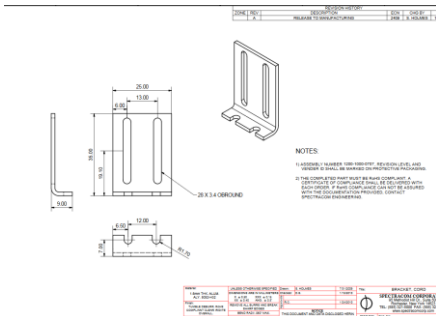


Partial Email from Dave Sohn (16 Sept 2020) Below is the parts list for the 1200-1000-0704 Rugged Ancillary Kit for SecureSync

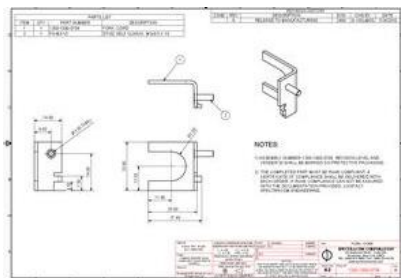
PART NO	QTY	DESCRIPTION
1200-1000-0706	2	Bracket, Rear
1200-1000-0707	1	Bracket, Cord
1200-1000-0708	1	Fork, Cord
HM11R-03R5-0004	2	Screw, PHP, M3-5, 18-8SS, 4mm, Thread Lock
HM20R-04R7-0010	4	Screw, FHP, M4, 18-8SS, 10mm, Black Oxide
HM72R-03R5-0002	1	Nut, Keps, M3 x 0.5mm, 18-8SS, 2.4mm HT

The 1200-1000-0707, 1200-1000-0708 are used to secure the AC power cord in the SecureSync using the two holes next to the power inlet module using (2) HM11R-03R5-0004 M3.5x4 screws and the HM72R-03R5-0002 nut.

- In addition to two rear support brackets, the AC support Bracket and hardware is included in the SecureSync Anc Kit, Rugged Installation" (1200-0000-0704)
- P/N for just the Power cord bracket 1200-1000-0707



- P/N for just the Power cord fork: 1200-1000-0708



- This cord bracket attaches to the two vertical holes right next to the AC power connector (using the two **HM11R-03R5-0004 screws**)



- SCREW, PHP, **M3-5**, 18-8SS, 4MM, THD LCK
- The thread size for these two holes in the SecureSync chassis are **M3** (not M3.5).

- **M3-5:** M3 screw with a .5 thread pitch (where the “M” stands for “metric”, and “3” is 3mm diameter)
- **18-8SS:** Made from 18-8 chrome/nickel stainless steel
- Length= 4mm
- **THD LCK:** thread lock?

Frequently Asked Questions (FAQs)

- 1) **EMI/EMC STANDARD: MIL STD 461F for submarine or STANAG 4370** does it match with SecureSync unit?
We tested the SecureSync for FCC part 15 and CE. We did not test against 461F or STANAG 4370, and have not done any analysis between the standards.
- 2) **Gravity Center of the equipment:** The SecureSync unit will have a RB option, 4 option boards and the fan will be replaced in the rear-left side of the unit (near GPS connector): Do you think I can say that the center of gravity stay in the center of the unit with this configuration or would you have some more precise answers on this subject ?

The SecureSync center of gravity changes with the options. With the AC power supply and Rb installed but no option cards. It will be forward of center and a little to the right (facing the front panel). If it's a DC only unit, it will be approximately in the center of the unit. Each option card added will move the center of gravity more to the left. The location of the fan will not significantly change the center of gravity, regardless of options.

Important Note: If mechanical/electrical modifications are made to the SecureSync appliance (such as relocating the fan) we can't guarantee compliance to our specifications. The specifications are generated based on the factory configuration of the equipment. Any modifications to the equipment may affect the specifications we provide.
- 3) **Regulation of the front panel lightning:** Is there any automatic regulation (for example against temperature variations) of the lightning of the front panel?
There is no automatic regulation of the front panel.
- 4) **Material, is it fungus resistant?** : do you have some information about the paint of the equipment (for example) that can allow us to say if the unit is well protected against moistures and fungus.
I have found a standard (MIL-V-173C), may be the customer wants some approached elements...
The SecureSync is not protected against condensing moisture and fungus at all. We would need to find anti fungus coatings for the boards and mechanical parts. These parts would have to be manufactured special for this order.

Associated questions from another customer (28 May 2020)

Are there any materials in SecureSync 1200 and the option card assemblies that are susceptible to mold/fungus? **Yes**

Is there any fungus/mold-proofing added to the components? **No**

- 5) **Ingress rating:** Refer to "IP rating/Ingress rating (for all products)" in the CustomerServiceAssistance document.

Any hazardous material internally? **None**

Do you have a material substance report? **No**

Fuses/Grounding / Input power (AC and DC) / Current

- Time servers are available as AC only, DC only, or one AC and one DC input
- Time servers are not directly available as two DC inputs or two DC inputs (but converters can be used external to the device).
- The two DC input ranges available are either:
 - 12vdc (10vdc -17vdc) OR
 - 24/48vdc (21vdc - 60vdc)

Power Fuses

A) DC input fuses

- Refer to “DC input power” further below

B) AC input power

- F010R-0002-000E, FUSE, 2A,SB, IEC SURGE, GLASS, 250V, 5X20M, Fuses for AC power entry module
- MFG P/N Littelfuse 0213002.MXP

The AC fuses (Spectracom P/N F010R-0002-000E) used in the SecureSync are from a company called Littelfuse and their P/N is 0213002.MXP. They are available through Digikey. They can refer to <http://parts.digikey.com/1/parts/692754-fuse-250v-iec-slo-5x20mm-2a-0213002-mxp.html> for replacements.



NATO code for the AC power fuse

Email from Sylvain (9 June 2015) I think I have found at least the little fuse NSN ref on the web site.
So it should be this one:

5920015888770 NSN CAGE 5FWY4
<http://buyaircraftparts.com/manufacturers/5FWY4>

Previous issues with fuses (ECN changes)

AC Fuses in SecureSync units sold before about 8/27/10:

ECN 2486 (~7/26/10) - SecureSync units were initially shipped with 4A instead of 2A fuses. This ECN changed the fuse to 2A. PSB2486 and new fuses were sent to all customers as of this time frame.

ECN 2517 (8/27/10) - SecureSync units with 208VAC input were popping the new 2A fuses. This ECN changed the two AC fuses to P/N F010R-0002-0000E. Only customers that reported the fuse blowing were sent replacements. No PSB was sent out. Units with the 2A fuse may see the fuses pop in the future because of too many power cycles. Then, supply customer with the fuses incorporated in ECN 2517.

Note: The correct fuses are small, 2 amp Slo Blow fuses. Manufacturer is “**Littelfuse**”. Their MFG P/N is **0213002.mxp**

Grounding

- Unlike NetClocks and Model 8195 series Master Oscillators, there is no dedicated rear panel grounding lug. Earth grounding is provided through the AC power cord or the DC connector (depending on which connectors are available and used).
- **Email from Dave Sohn (22 April 2020)** For those customers that do want to utilize a ground strap, we generated this document (copy pasted below) Refer to "I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Input power and grounding\Grounding"



A) Default grounding info/EGC/Safety

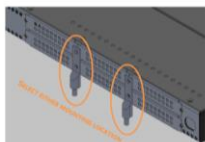
Default Grounding Information

SecureSync 1200 provides default safety grounding through our standard AC and/or DC power connectors. The AC and DC power connectors include an equipment grounding conductor (EGC), which is connected internally to the equipment chassis for safety grounding. The SecureSync 1200 safety certification is achieved by utilizing these power connectors and a power cable also including an appropriate EGC.

B) Attaching optional ground strap to chassis

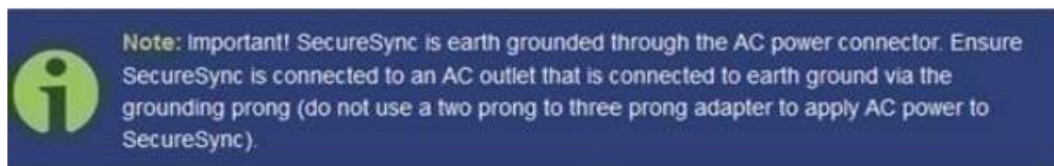
Optional Grounding Information

For customer installations that wish to utilize a separate safety earth ground connection, there is no specifically marked safety earth ground location on the SecureSync 1200. However, additional earth grounding can be achieved by utilizing the option card mounting holes between columns of option cards on the rear of the unit as shown in the figure below. Either location is suitable to provide additional grounding utilizing standard two-hole lugs with 1/4" spacing for #10 bolts (e.g. Bundy pj yaki-2ic10e2). The standard M3x6mm option card mounting screws should be replaced with 7mm OD flat washers and M3x6mm mounting screws to properly attach the lugs. If labeling is desired, a Earth Ground label (e.g. My Safety Label pin LB-0609) should be affixed to an adjacent option card plate.

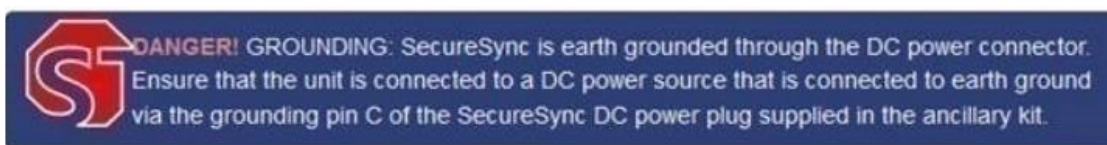


Q Need to connect ground strap to SecureSync unit installed in a cabinet. But the information is not in any of the posted install guides. Can you please provide guidance on proper hardware for attaching a ground for the unit to the cabinet.

A As excepted below from the online SecureSync user guide, **for AC input** power (http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INSTALL/AC_pwr.htm):



And as excepted below from the online SecureSync user guide **for DC input** power (http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/INSTALL/DC_pwr.htm):



Unlike some of our earlier Model products, having an external ground lug cable connection for attaching a ground to the chassis, as the SecureSync's chassis is grounded via its power connection, the SecureSyncs do not need to/nor provide a ground lug for external grounding.

If for some reason you have a requirement to add an additional earth ground connection to the chassis (note that we have been selling SecureSyncs to Raytheon for several years now, and this is the first inquiry we've ever received from your organization about adding a separate ground to the chassis) the paint would need to be removed and a custom ground lug attached to the chassis. Because of the chassis grounding already provided, we don't have any recommendations/methods available on adding additional custom grounding.

Per the notes above indicating how the chassis is already grounded via its power connections, I would be surprised to hear a need to provide a second ground connection to the chassis.

F/U Email from Dave Sohn (22 April 2020) For those customers that do want to utilize a ground strap, we generated this document (see link further above)

Input power

**Power monitor / alarms / traps

Refer to the response to our dealer in Salesforce Case 290132

- There are no Alarms (or the front panel Fault LED) associated with a loss of one power source, when the unit is configured for dual (both AC and DC) input. Since there are no alarms associated with input power loss, there are also no traps associated with power in the 1200s.
- An indicator change (the color of the front panel POWER LED) is provided when both AC and DC input connectors are present, but one of the two inputs is not present.
 - Refer to https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/INTRO/Fro_Pa_StatLEDs.htm

Front panel status indications

LED Label	Indication	Description
POWER	Off	Both AC, and DC input power are disconnected. OR: The unit's AC input switch is turned OFF, and DC input is not present.
	On/solid green	AC and/or DC Power are supplied; the unit detects all power inputs.
	Red	The unit is configured for two power inputs, but detects only one power input. OR: Detects a power configuration error.
	Green & blinking orange 1sec.	Power Error — general power configuration fault.

- For more info, refer also to: ****Front panel status LEDs/ (AC and DC power monitoring)** in this document.

Alert notification (such as SNMP traps) for loss of redundant power

- As of at least software version 5.9.5 and below, there are no Alarms/Fault SNMP traps associated with loss of redundant power (and at this point I HIGHLY doubt there ever will be)
 - Refer to Mantis case 3064 (25 June, 2015) regarding a request for SNMP trap capability to be added.

A) AC power

- Refer to online user manual at: http://manuals.spectracom.com/SS/Content/NC_and_SS/SS/Topics/INTRO/Specs_InputPower.htm

AC switching power supply data sheets

- Link to DC to DC converter data sheets: I:\Engineering\Engineering Shared\Spectracom Parts ROHS\PS03R-xxxx-xxxx (TDK-Lambda)

Phase: Single phase

AC input Voltage

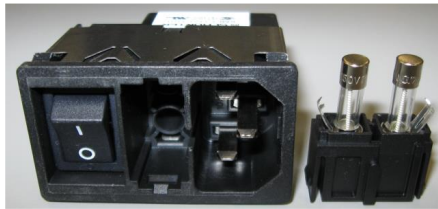
Either:

1. 100-240VAC at 50/60 Hz (+/- 10% for both voltage and frequency)

- **Note:** SecureSync can actually accept **90 to 264VAC**, but we state 100-240VAC for UL requirements.
- **Note:** SecureSync can actually accept **45 to 66 Hz**, but we state 50/60 Hz for UL requirements

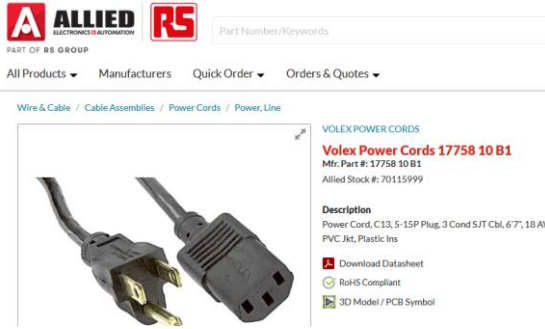
2. 100-120VAC at 400 Hz (+/- 10% for both voltage and frequency)

AC power connector: Unit has C14 inlet connector



AC line cords for 240VAC input to the C14 connector on back of the 1200 SecureSyncs

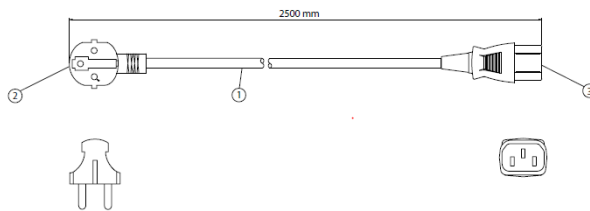
- Refer to Salesforce Case 285021
- As of at least May 2022, I don't believe we offer any 240VAC input line cords.
- Customers need to 'locally obtain' a 240VAC to C13 line cord. Some suggested Sources/Part Numbers below:
 - Mouser Electronics (<https://www.mouser.com/c/?q=AC%20line%20cords>)
 - Quail Electronics, inc (https://www.quail.com/typesearch.htm?type=plugreceptaclematrix&gclid=CjwKCAjwp7eUBhBeEiwAZbHwkW56yg9zYZdkifvJC0cKGKX4KqLd33egbQr6lDeiTphmWwPIYLrXwBoC4z8QAvD_BwE)
 - Walmart (confirm with Eng) : <https://www.walmart.ca/en/ip/Tripp-Lite-P032-007-7-Foot-AC-Power-Cord-10A-100-240V-12Awg-C13-C20/PRD6SHG20D8DNU>



- Refer to “**RoHS compliancy statement for SecureSyncs and 9400s**” in this same document

B) Euro version line cord (CA06R-EU13-0001)

- Our P/N: CA06R-EU13-0001 (in Arena) https://app.bom.com/items/detail-spec?item_id=1203165790&version_id=10257870248
- **Description:** AC CORD,EU to C13,18AWG,10A,250V, 70C
- **Cable length:** 8.2 feet (2500 millimeters)



PLUG: CONTINENTAL EUROPEAN CEE 7 RIGHT ANGLED **Connector:** IEC 60320 C13 (to SecureSync)

Note: As of at least March 2015, we don't offer any alternate AC power cables (such as a C13 to C14 cable for example) and Dave Sohn doesn't want to get into supporting various other power cables. The C13 to xxx cables should be readily available locally.

Power cords for Les Ulis that will work with SecureSync if one is not specified and shipped with the order **Per Tom Richardson - cord for STA or CNT-90 would work.**

Input power signal characteristics/requirements (Sinusoidal power/ square wave power)

- Refer to: [Power interruption tolerance: UPS backup to AC input for SecureSyncs/9400s](#)

Input AC current (amps)/power (watts)

Email from Mark McGregor

The amps drawn depends on the input voltage, that is why power draw is specified.

The amps drawn will be roughly the power drawn divided by the AC line voltage ($P=VI$, $I=P/V$). For example, we specify 40W normal for an OXCO. If the AC power is 115VAC, the current draw is $40W/115VAC \approx 0.35Amp$. This would only be when the customer had all six option cards installed; it should typically be less than that.

The AC input is rated for 1A maximum, but that is at low AC voltage of 90VAC, and the 1A has at least 20% margin over what the box actually draws, to ensure the maximum is never exceeded, as it is a safety parameter.

Another Email from Mark McGregor (17 Jan 2013)

Note: Mark also included MFG data sheets for the TDK-Lambda and TDK Lambda LS100 evaluation test dat **Refer to:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Input power>

It is really just taken from the specification of the AC to DC power supply, as a maximum. It also depends on the AC line voltage and the AC fuses and the chassis wiring. The AC to DC power supply specifies it as 60A maximum with 277VAC input voltage. SecureSync uses an LS100-12 power supply. See attached data sheet and evaluation test data.

I think that the actual value would be lower due to the SecureSync chassis wiring and the slow blow AC fuses that are IEC surge rated.

We also do not have equipment to measure it. We would have to rent equipment, or send a unit somewhere, or take it somewhere that does have that equipment to know what the actual number is.

Q "I'm looking for some technical data on the SecureSync GPS (P/N 1200-003). Can you provide me with the following information:

- 1) Maximum Current draw for 115VDC and 220VDC voltage sources.
- 2) Maximum Power Consumption for 220VDC voltage sources.
- 3) Heat Dissipation for 115VDC and 220VDC voltage sources.

A Reply from Tom R (15 sept 17)

Data Sheet Page 3

TCXO: 40W normal (50W startup)

- 1) Maximum Current draw for 115VDC and 220VDC voltage sources.
- 2) Maximum Power Consumption for 220VDC voltage sources. 50 Watts
- 3) Heat Dissipation for 115VDC and 220VDC voltage sources. 50 Watts

Watt = 1VRMS * 1A therefore Amp = Watt/VRMS

50 Watts/115VRMS = 0.43 A

50W/220V = 0.23 A

AC Power Factor/ Power draw

AC Power Factor

- Refer to case 24906
- measured Power Factor of an AC unit in the lab was + 0.83 (valid range for power factory is from -1 to +1).

from https://en.wikipedia.org/wiki/Power_factor

In electrical engineering, the **power factor** of an AC electrical power system is defined as the ratio of the real power flowing to the load to the apparent power in the circuit, and is a dimensionless number in the closed interval of -1 to 1 . A power factor of less than one means that the voltage and current waveforms are not in phase, reducing the instantaneous product of the two waveforms ($V \times I$).

Q Email Keith sent to Tom Richardson: In reference to our Salesforce case 24906 (submitted by Jim Rayhill with Harris), he is asking for the “Power Factor” for SecureSync’s AC input...
I looked in my notes and the SecureSync online manual, but wasn’t surprised it’s not mentioned in either place (believe this is the first time I’ve heard it asked for this product)

A (response from Tom Richardson, 31 Mar 17) I measured Power Factor of an AC unit in the lab and got 0.83.

Volt-amps (VA)

Q Could you please give us the requirement of following specification?
Unit: 1200-033
Spec: Apparent electric power (VA)

According to the datasheet, the SecureSync(033) need 80W at bootup, and 50W at actual use.
The customer wants to know also VA values to calculate load of their power supply.

A Reply from Josh (based on info he received from Jean-Arnold) 16 Jan 18: The Apparent electric power for the SecureSync is as follow :

55.5VA at actual use
88.9VA at boot up.

Power draw (from Data Sheet)

- **TCXO:** 40W normal (40W start-up)
- **OCXO:** 40W normal (50W start-up)
- **Rb:** 50W normal (80W start-up)

Attached you should find a copy of the SecureSync data sheet. Page 3 (second to last page) contains the “Power Draw” specs for SecureSync. The power draw that will exist with SecureSync is primarily based on which type of oscillator is installed in the appliance (the TCXO, OCXO or Rubidium oscillator).

The oscillators inherently draw more current when they are cold, so the start-up wattage is higher than is during normal operation (as shown in the above specs). Once the oscillators have become internally warm again, the power draw by the oscillator is able to drop.

Not only will the type of oscillator affect the power draw, the specific configuration of the installed Option Cards will also affect the amount of power draw, as well. These specs in the datasheet are the maximum power expected in any configuration of the option cards. I spoke to one of our engineers that performed the measurements for these specs and he said the power draw difference between the AC input and DC input is negligible (as your customer is asking about).

The engineer also mentioned that when powering SecureSync with both AC and DC input power (for automatic failover upon loss of AC power to DC power), even though the DC power is not being used when AC power is present, there is still a few watts drawn on the DC power as its used by the DC to DC converter.

Two Emails from Mark McGregor:

We do not/did not measure the current draw for each option card configuration. It will be less than the data sheet maximum of 1A. I came up with the data sheet value using 20W of option card power draw with power resistors to simulate the option cards, and I am sure it is less than that.

I measured about 0.7A for the Rubidium (033) at start-up with 20W simulated option card load, and added some margin to get 1A. I can't say how much less, as I don't know what a 1204-05 option card draws, as that is a SAASM option card we are not allowed to have. I do not know how much power a 1204-06 Ethernet card draws.

I found the data I took. It was on 11/23/2009. I used a low AC line voltage of 95V (draws more current than 115V) in a model 033 Rubidium with AC power SecureSync, with 20W of extra load to simulate option cards

At start up, the current draw was 0.75A at 95VAC.

After 3 minutes the current dropped to 0.5A at 95VAC

After 20 minutes, the current was 0.47A at 95 VAC.

With AC line at 115V, current drop rflowers@murphymedical.org ed to 0.40A.

The unit shipped to the customer will be somewhat less than this.

208 VAC input with both being hot with respect to ground

Email from Mark McGregor (5/23/11) The SecureSync will run OK from 208VAC, two phases of the three phase power, but they must still supply an earth ground on the third pin of the AC power connection for the SecureSync to remain safe per UL60950-1 and CE EN60950-1 safety standards. The SecureSync is rated for 100-240VAC up to 2000 meters of altitude. As long as Tony's customer is not going to operate the product above 2000m, then 208VAC is OK when an earthed ground is supplied on the third pin of the SecureSync AC power inlet.

FYI - The 208V is derived from using two lines of the 120V three phase power. Each phase voltage is 120VAC, but when two of them are used together, due to them being 1/3 of a cycle (120 degrees) out of phase with each other, the result is 208VAC. This is what the IT data centers are doing that were blowing the AC fuse that did not have a high enough surge rating.

In order to comply with UL and CE safety both AC lines must be treated as being potentially hot. Neither AC line can go directly to earth ground.

The reason for the double pole/neutral line fusing, is that if one of the incoming AC lines can't be reliably identified as an earthed neutral, then both sides of the AC line must be fused, if fusing is used for overcurrent protection. In the US consumer 120V outlets, the one AC slot being wider than the other identifies the earthed neutral, so only one fuse is required in the known "hot" line. In Europe, they don't have this kind of outlet, so you can't guarantee that one of the two lines is an earthed neutral, so both must be fused.

Power interruption tolerance: UPS backup to AC input for SecureSyncs/9400s

- Current draw of the oscillator should be considered when selecting a UPS to use with SecureSync
- Refer to the following about email below: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\UPS for SecureSync>

- The SecureSync can operate for up to 20 msec. after AC input power is lost with no negative effects.

Q They are planning to prepare some measures for instantaneous interruption of their power supply. Could you please tell us how much variation can the power unit of the time server allow?

They want to confirm following specifications of the time server:

- Allowable voltage drop threshold [V]
- Allowable instantaneous interruption period [sec]

A Email from Dave L (14 Feb 18) Per the user manual, the SecureSync can operate for up to 20 msec. after AC input power is lost with no negative effects

Questions from SF case 126365

1. We are trying to support a Securesync unit on a UPS. One UPS we have in mind would have a brief power interruption when switching from primary power to battery power, rated to be between 4 and 8 milliseconds. Question is this: What are the capabilities of the Securesync unit to ride through such a power interruption? What power interruption can it ride through without losing time (under the assumption that GPS is not available and the unit is running on an internal Rb standard)?

1a. Does the unit require sinusoidal power? Or is it OK with square wave power some UPS's output?

A Reply from Mark McGregor (7 Feb 18) The AC power supply internal to SecureSync is a TDK-Lambda LS100. It has a hold up time specification, which is how long it can operate after loss of AC power. LS100 hold up time is 25 msec typical with 115 VAC input, and 150 msec. typical for 230VAC input. That being the case I would tell the customer that SecureSync can operate for 20 msec. after AC input power is lost since the TDK spec is "typical", not minimum. If power is restored less than 20 msec after it is lost, the SecureSync should not experience a power cycle, restart.

As far as the AC input waveform, it is not specified for the TDK-Lambda LS-100. The AC input is specified as 88VAC to 264VAC RMS at 47-63 Hz frequency. It can operate with DC input from 125V to 373V DC. I think that a square wave would work if its AC RMS voltage is within 88 to 264 VAC, at 47 to 63 Hz frequency. An inquiry could be made to TDK-Lambda local sales rep to try to get an answer from TDK-Lambda.

Q from Mike Messina to Tom Richardson referring to FAA: Any idea of what they can use as a UPS now with SecureSync?

A Reply from Tom R (30 May 17) A 12 to 36 VDC backup supply should work. Try this.
<http://www.technologydynamicsinc.com/dc-ups/tdrsp-1urk-bbu12-50.php>

- Q Site where Time Server is located has regular testing where they fail over from one power source to another. Since the Time Server only has one power supply, this will take the Time Server down regularly. Do you have an option for a secondary power supply that can be plugged into a separate PDU? or do you supply/recommend a small UPS for short power outages?

A (reply from DL 16 Feb 18) Answer:

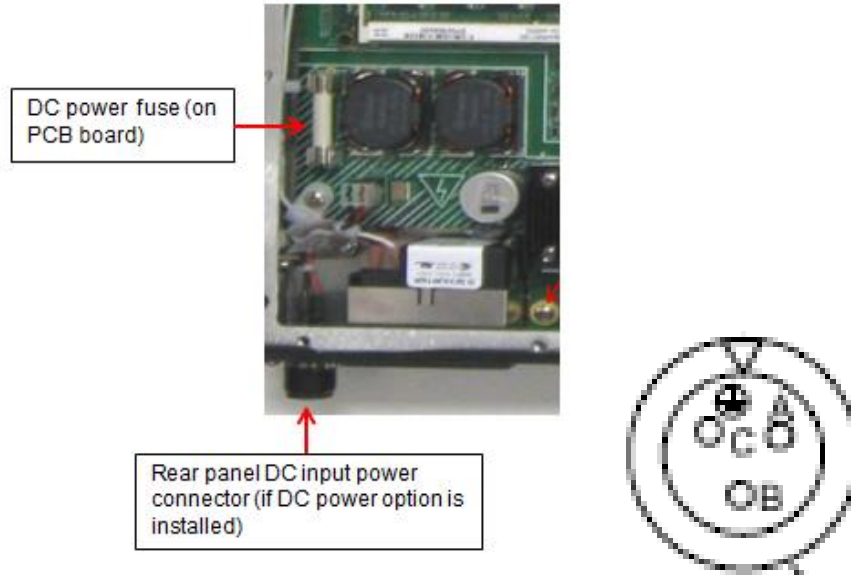
The Securesync does have a dual power option but this must be ordered at the time of purchase. It is not installable afterwards.

The best method of protection from power outages for this Securesync is to use a UPS system.

The size of the UPS depends on what the oscillator option is on your Securesync

- TCXO: 40W normal (40W start-up)
- OCXO: 40W normal (50W start-up)
- Rb: 50W normal (80W start-up)

B) DC input power



1. 12vdc (or -12vdc) input power

- Spectracom Fuse P/N F030R-0010-000E, FUSE, 10A, FB, CERAMIC CART,250V,3AB, 12VDC power fuse
- **MFG P/N** Littlefuse 0314010.HXP or 0314010.MXP
- **DC power jack** (included in "DC" and "AC/DC" anc kits: our P/N P240R-0032-002f (in Arena) at https://app.bom.com/items/detail-spec?item_id=1202844982&version_id=10221223528)
- DC ripple:

2. 24/48vdc (or -24vdc / -48vdc) input power

- Spectracom Fuse P/N F030R-0005-010E, FUSE, 5A, FB, CERAMIC CART,250V,3AB, 24/48VDC power fuse
- **MFG P/N** Littlefuse 0314005.HXP or 0314005.MXP
- **DC power jack** (included in "DC" and "AC/DC" anc kits: our P/N P240r-0032-002f (in Arena) at: https://app.bom.com/items/detail-spec?item_id=1202844982&version_id=10221223528)
- DC ripple:

DC input Pinout info

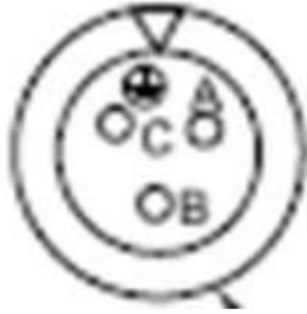
The SecureSync/Model 9483 is capable of operating on:

- **Both +12vdc and -12vdc** (when the 12vdc input Option is installed),
- **Both +48vdc and -48vdc** (when the 24/48vdc input Option is installed).

Refer to the online NetClock Model 9483 ("**Using DC Input Power Section**") at:

http://manuals.spectracom.com/NC/Content/NC_and_SS/Com/Topics/INSTALL/DC_pwr.htm.

At the bottom of this page, click to expand the "**Pinout description, DC connector**" information. As also excerpted below, the NetClock can accept either + or - DC input voltage. The difference between the two is just which Pin (Pin A or Pin B) of the three pin connector the DC power is connected to:



Pin B goes to the most positive DC voltage of the DC source. For +12 V or +24/48 V this would be the positive output from the DC source. **For a -12 V or -24/48 VDC source this would be the ground or return of the DC source.**

Pin A goes to the most negative voltage of the DC source. For +12 V or +24/48 V this would be the ground or return output from the DC source. **For a -12 V or -24/48 VDC source this would be the negative output from the DC source.**

Pin C goes to the Earth ground of the DC source.

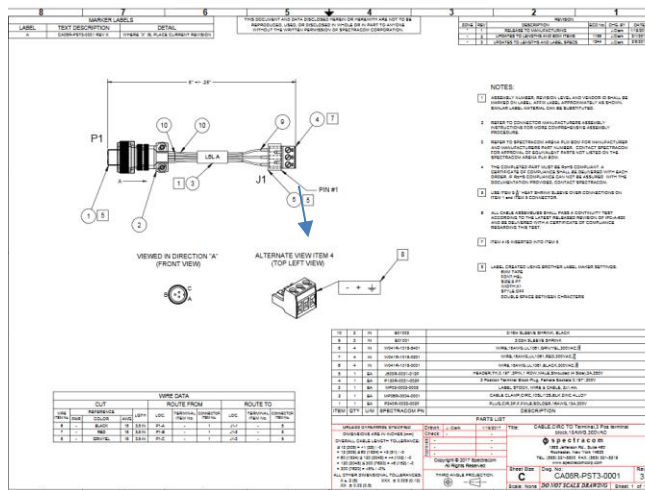
Secure locking DC input connector (attaches to DC input jack on rear panel)

- (included in “DC” and “AC/DC” anc kits: our P/N **P240R-0032-002F** (in Arena) at: https://app.bom.com/items/detail-spec?item_id=1202844982&version_id=10221223528)
- Refer to “Secure locking device” further below for additional info on this connector

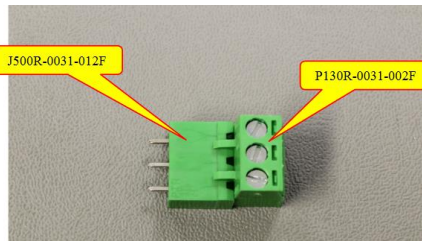
CA08R-PST3-0001 (DC connector to 3 position terminal block connector adapter cable)



- **Description:** CABLE,CIRC TO Terminal,3 Pos terminal block,18AWG,300VAC
- **in SAP:** https://app.bom.com/items/detail-spec?item_id=1223896303&version_id=10709212858
- **Process Detail (CA08R-PST3-0001-PD) in Arena:** https://app.bom.com/items/detail-spec?item_id=1248910025&version_id=11027259628
 - PD includes the drawing below



3 Pin Terminal block connector (plugs into J500R-0031-012F, which is soldered to the wires)



Note: The three Wires are soldered onto the small metal shafts and shrink-wrapped onto a separate Jack (there are two connectors, not just one).

Our P/N: P130R-0031-002F

MFG and MFG P/N: On Shore ED950/3

DigiKey P/N: ED1702-ND <https://www.digikey.com/product-detail/en/on-shore-technology-inc/ED950-3/ED1702-ND/123765>

Desire to convert a DC only unit to AC input power

Highly recommend considering to purchase and use the [Spectracom Model PS06R-2Z1M-DT01 \(Available AC to 24VDC converter for redundant AC input\)](#) instead of retrofitting the time server. This external AC to DC converter will alleviate the need for the equipment to be returned to us for hardware modifications.

Q. (from Scott Holmes to Mark McGregor) There is a 10A fuse located on the SecureSync main board near the DC supply area. Do we consider that a “field replaceable” part?

A. Reply from Mark McGregor (10/24/12) The 10A fuse is only used for the 12V DC option. There is a 5A fuse that goes in the same spot for the 24/48V DC option. That fuse is not populated if no DC input option is present.

I am fairly sure that none of the parts inside the box are considered to be field replaceable for UL safety. (Keith’s edit- Refer to the SecureSync manual for more info).

Known issues

- 1) **NC 6111/CA 883 (5 Sept 2012):** CA08R-PSMT-0001 cable was being made with the wrong connector, resulting in grounding issues. I spoke to Dave Sohn today. He said no PSB is required for this issue, was addressed with the cable supplier.

C) SecureSyncs with both AC and DC Input power



Note: AC input, when supplied, is selected over the DC input (AC input is primary. DC input is backup).

Altitude limitations for the internal power supply (AC and DC)

- Refer to the SecureSync data sheet
- SecureSync Data Sheet lists both 100-240 VAC to 6,560 feet and 100-120 VAC to 13,123 feet
- Per Dave Sohn- Max altitude for DC power is same as 100-120 VAC... 13,123 feet.

Environmental

	Operating	Storage	MIL-STD-810F
Temperature	-20 to +65°C (+55°C for Rb)	-40 to +85°C	501.4, 502.4
Humidity	0%-95% RH non-condensing @ 40°C		507.4
Altitude	100-240 VAC to 6,560 ft (2,000 M), 100-120 VAC to 13,123 ft (4,000 M) 12-17 VDC and 21-60 VDC to 13,123 ft (4,000 M)	45,000 ft (13,700 M)	500.4
Shock	15g/0.53oz, 11ms half sine wave	50g/1.76oz, 11ms half sine wave ¹	516.5
Vibration	10-55Hz/0.07g, 55-500Hz/1.0g	10-55Hz/0.15g, 55-500Hz/2.0g	514.5

Associated AC and DC input power Ancillary Kits:

1) P/N 1200-0000-0702 (ANC KIT, SECURESYNC, N.AMER, AC & DC OPT)

- in Arena at: https://app.bom.com/items/detail-bom-flat?item_id=1203165692&version_id=10299428868&&redirect_segno=17898661621
- Description in Salesforce: “SecureSync Anc Kit, AC/DC for North America including: Front rack ears Handles Mounting hardware AC power cord (NEMA 5-15P to C13) DC power connector and cable clamp”

#	ITEM NUMBER	ITEM NAME	CATEGORY		
1	1165-1000-0714 rev D	9383, RACK EAR	Fabricated Metal	1	2 EA
2	1200-1006-0802 rev 1	ANC KIT LABEL, SECURESYNC, N.AMER, AC & DC OPT	Label	2	0 EA
3	CAD0R-1513-0001 rev 2	AC CORD 5-15P to C13,18AWG,10A,125V,10SC	Cable Assembly	4	1 EA
4	H020-0832-0406 rev 1	SCREW,FHP,B-32,18-8SS,3/8in, BLACK-OXIDE	Fasteners/Spacers, Unified	1	4 EA
5	HM20R-04R7-0010 rev 1	SCREW, FHP, M4, 18-8SS, 10MM,BLACK OXIDE	Fasteners/Spacers, Metric	1	6 EA
6	MP02-0003-0002 rev 2	LABEL STOCK, 6 UP	Label	1	0 EA
7	MP06R-0004-0001 rev 1	CABLE CLAMP,CIRC,105L/125,BLK,ZINC ALLOY	Miscellaneous Mechanical	1	1 EA
8	MP09-0003-0030 rev 1	HANDLE, WIRE PULL, 30MM	Miscellaneous Mechanical	1	2 EA
9	P240R-0032-002F rev 1	PLUG,CIR,3P,F,FMIL,B,SOLDER,16AWG,13A,300V	Plug	1	1 EA

2) P/N 1200-0000-0712 (ANC KIT, SECURESYNC, AC & DC OPT)

- in Arena at: https://app.bom.com/items/detail-whereused?item_id=12211034397&version_id=10565694548&orb_msg_single_search_p=1
- Description in Salesforce: “SecureSync 1200 Anc Kit, AC/DC including: Front rack ears, Handles, Mounting hardware, DC power connector and cable clamp (not compatible with SecureSync 2400)”

#	ITEM NUMBER	ITEM NAME	CATEGORY		
1	1165-1000-0714 rev D	9383, RACK EAR	Fabricated Metal	1	2 EA
2	1200-1006-0812 rev 2	ANC KIT LABEL, SECURESYNC, AC & DC OPT	Label	2	0 EA
3	1200-5000-0051 rev 12	QUICKSTART GUIDE, SECURESYNC	Manual	1	1 EA
4	H020-0832-0406 rev 1	SCREW,FHP,B-32,18-8SS,3/8in, BLACK-OXIDE	Fasteners/Spacers, Unified	1	4 EA
5	HM20R-04R7-0010 rev 1	SCREW, FHP, M4, 18-8SS, 10MM,BLACK OXIDE	Fasteners/Spacers, Metric	1	6 EA
6	MP02-0003-0002 rev 2	LABEL STOCK, 6 UP	Label	1	0 EA
7	MP06R-0004-0001 rev 1	CABLE CLAMP,CIRC,105L/125,BLK,ZINC ALLOY	Miscellaneous Mechanical	1	1 EA
8	MP09-0003-0030 rev 1	HANDLE, WIRE PULL, 30MM	Miscellaneous Mechanical	1	2 EA
9	P240R-0032-002F rev 1	PLUG,CIR,3P,F,FMIL,B,SOLDER,16AWG,13A,300V	Plug	1	1 EA

D) DC input power

- **Note:** AC input, if supplied, is selected over DC input (AC input is primary. DC input is backup).

DC to DC converter installed

1. **12Vdc (or -12vdc) Option range: 10- 17vdc**
 - Uses DC to DC converter P/N PS03R-0J0J-PC00(8 Amps)

Note: This DC to DC converter can actually handle 10 to 22vdc input, but we specify 10 to 17vdc with a tolerance for UL requirements

Our P/N: PS03R-0J0J-PC00 (in Arena at https://app.bom.com/items/detail-spec?item_id=1202845980&version_id=10221213338&orb_msg_single_search_p=1)

MFG and P/N: SYNQOR IQ12120QTC10NRS-G

IQ12018QTC40 ELECTRICAL CHARACTERISTICS (1.8 V_{OUT})

T_A = 25 °C, airflow rate = 300 LFM, V_{IN} = 12 V_{DC} unless otherwise noted; full operating temperature range is -40 °C to +100 °C ambient temperature with appropriate power derating. Specifications subject to change without notice.

Parameter	Min.	Typ.	Max.	Units	Notes & Conditions
INPUT CHARACTERISTICS					
Maximum Input Current			13.0	A	9 V _{IN} trim up; in current limit
No-Load Input Current		314	600	mA	
Disabled Input Current		2.0	4.0	mA	
Response to Input Transient		0.2		V	250 V/ms input transient; 100 µF output cap.
Input Terminal Ripple Current		168		mA	RMS
Recommended Input Fuse			30	A	Fast acting external fuse recommended
Input Filter Component Values (L/C)		0.47/24		µH/µF	Internal values; see Figure E
OUTPUT CHARACTERISTICS					
Output Voltage Set Point	1.782	1.800	1.818	V	
Output Voltage Regulation			25	mV	Full Load
Over Line		+0.1	+0.3	%	
Over Load		+0.1	+0.3	%	
Over Temperature	-27			mV	
Total Output Voltage Range	1.755		1.845	V	Over sample, line, load, temperature & life
Output Voltage Ripple and Noise 1					20 MHz bandwidth
Peak-to-Peak		82	160	mV	Full Load
RMS		14	25	mV	Full Load
Operating Output Current Range	0		40	A	Subject to thermal derating
Output DC Current-Limit Inception	44		52	A	Output Voltage 10% Low
Output DC Current-Limit Shutdown Voltage		0.9		V	
Back-Drive Current Limit while Enabled		0.3		A	
Back-Drive Current Limit while Disabled	0	15	50	mA	Negative current drawn from output
Maximum Output Capacitance			10,000	µF	Negative current drawn from output
Output Voltage during Load Current Transient		90		mV	50% to 75% to 50% I _{OUT} max
For a Step Change in Output Current (0.1 A/µs)		200		µs	To within 1% V _{OUT} nom
Setting Time					Measured across Pins 8 & 4; Common Figure 3
Output Voltage Trim Range	-20		+10	%	Measured across Pins 8 & 4
Output Voltage Remote Sense Range			+10	%	Measured across Pins 8 & 4
Output Over-Voltage Protection	117	122	127	%	Over full temp range; % of nominal V _{OUT}
Load Current Scale Factor		2667		%	See Output Load Current app. note on our web
EFFICIENCY					
100% Load		82		%	See Figure 1 for efficiency curve
50% Load		83		%	See Figure 1 for efficiency curve

2. 24/48Vdc (or -24/-48vdc) Option range: 21-60vdc

➤ Uses DC to DC converter P/N: **PS03R-1U0J-PC00** (10 Amps)

Note: This DC to DC converter can actually handle 18 to 75 vdc input, but we specify 21 to 60vdc with a tolerance for UL requirements

Our P/N: PS03R-1U0J-PC00 (in Arena at https://app.bom.com/items/detail-spec?item_id=1202845981&version_id=10228388768&orb_msg_single_search_p=1)

MFG and P/N: SYNQOR IQ36120QTC10NRS-G

IQ36 FAMILY ELECTRICAL CHARACTERISTICS (all output voltages)
T_A = 25 °C, airflow rate = 300 LFM, V_{IN} = 36 V_{DC} unless otherwise noted; full operating temperature range is -40 °C to +100 °C ambient temperature with appropriate power derating. Specifications subject to change without notice.

Parameter	Min.	Typ.	Max.	Units	Notes & Conditions
ABSOLUTE MAXIMUM RATINGS					
Input Voltage			80	V	Continuous
Operating Transient Protection			75	V	Continuous
Isolation Voltage			2550	VDC	Not applicable
Input to Base-Plate			2550	VDC	Basic insulation, Pollution Degree 2
Output to Base-Plate			2550	VDC	
Operating Temperature	-40		100	°C	Baseplate temperature
Storage Temperature	-55		175	°C	
Voltage at ON/OFF input pin	-2		18	V	
INPUT CHARACTERISTICS					
Operating Voltage Range	18	36	75	V	Not applicable
Input-On Voltage Threshold	16.6	17.0	17.4	V	
Turn-Off Voltage Threshold	15.0	15.4	15.8	V	
Lockout Voltage Hysteresis		1.6		V	
Recommended External Filter Capacitance		220		µF	Typical ESR 0.1-0.2 Ω
DYNAMIC CHARACTERISTICS					
Turn-On Time		9		ms	Full load, V _{IN} 90% nom.
Start-Up Inrush Time	200	200	250	ms	See Figure F
Output Voltage Overshoot				%	Maximum Output Capacitance
ISOLATION CHARACTERISTICS					
Isolation Voltage (electric strength)		30		MO	See Absolute Maximum Ratings
Isolation Resistance		1000		µF	
TEMPERATURE RANGES/DERATING					
Semiconductor Junction Temperature		125		°C	Package rated to 150 °C
Board Temperature		125		°C	UL rated max operating temp 130 °C
Transformer Temperature		125		°C	See Common Figure 3 for derating curve
Maximum Baseplate Temperature, T _B		100		°C	
FEATURE CHARACTERISTICS					
Switching Frequency	330	350	370	kHz	Regulation and Isolation stages
ON/OFF Control			18	V	
On-State Voltage	2.4		0.8	V	
ON/OFF Control	-2			V	Common Figures A & B
Full-Load Voltage		5		V	
Pull-Up Resistance		50		Ω	
Over-Temperature Shutdown		100		°C	Average PCB Temperature
Over-Temperature Shutdown Restart Hysteresis		10		°C	
RELIABILITY TESTS					
Qualification MTBF (MIL-STD-883C, HWY-000132)		2.5		10 ⁶ hrs	80% load, 1000 RPM, 40 °C T _A
Calculated MTBF (MIL-STD-217F, MIL-HDBK-217F)		2.0		10 ⁶ hrs	80% load, 1000 RPM, 40 °C T _A
Field Demonstrated MTBF				10 ⁶ hrs	See our website for details

DC input Pinout info

The SecureSync/Model 9483 is capable of operating on:

- **Both +12vdc and -12vdc** (when the 12vdc input Option is installed),
- **Both +48vdc and -48vdc** (when the 24/48vdc input Option is installed).

Refer to the online NetClock Model 9483 (“Using DC Input Power Section”) at: http://manuals.spectracom.com/NC/Content/NC_and_SS/Com/Topics/INSTALL/DC_pwr.htm.

At the bottom of this page, click to expand the "Pinout description, DC connector" information. As also excerpted below, the NetClock can accept either + or - DC input voltage. The difference between the two is just which Pin (Pin A or Pin B) of the three pin connector the DC power is connected to:



Pin B goes to the most positive DC voltage of the DC source. For +12 V or +24/48 V this would be the positive output from the DC source. **For a -12 V or -24/48 VDC source this would be the ground or return of the DC source.**

Pin A goes to the most negative voltage of the DC source. For +12 V or +24/48 V this would be the ground or return output from the DC source. **For a -12 V or -24/48 VDC source this would be the negative output from the DC source.**

Pin C goes to the Earth ground of the DC source.

DC Ripple spec (for 21- 60vdc input): 260mA RMS

Amps/Watts for 48vdc

Q ...We are working on putting together some information in a bid that requires details surround the Securesync 48V electrical specs. Your website provides details on the AC, 120V side.

Could you provide me the following specs for the 48V DC operations:

- DC Amps
- DC Power
- Recommended DC breaker size (if you have one)
- Thermal contribution (in BTU)

Email from Tom Richardson (25 Sept 17) The information you have is correct as far as I know.

DC amps would be calculated as the Watts divided by the Voltage.

We have no recommended DC breaker size.

We have not measured or calculated the Thermal contribution in BTU.

A Reply from Jodi to Customer

Here are the answers, below, to your questions about the SecureSync.

DC input (option):

- 12-17 V_{DC} -15%, +20%, or
- 21-60 V_{DC} -15%, +20%, secure locking device

Maximum power draw:

- TCXO/OCXO oscillator installed: 40 W normal (50 W start-up)
- Rubidium (Rb) oscillator installed: 50 W normal (80 W start-up)
- Low-Phase Noise (LPN) Rubidium oscillator installed: 52 W normal (85 W start-up)

We have no recommended DC breaker size and we have not measured or calculated the Thermal contribution in BTU. I do have some information on the cooling fan and thermal dissipation that may help, however:

- Rb oscillator: 50W normal (80W start-up) 170.60708165 BTU/hr normal, (272.97133064 BTU/hr startup) Startup time is 30 minutes.

The cooling fan: Air flow: 1.30 CFM

SecureSync Chassis Cooling: The cooling fan, while running (it is temperature controlled), pulls ambient air in through the right side of the front panel. The chassis was intentionally designed to have holes only on the back of the left side of the chassis, so air is essentially “ducted” to and across the back end of the chassis for cooling (drawing heat away from the components located towards the front of the chassis).

Second reply from Jodi (25 Sept 17)

I also have this information. Let me know if it's what you're looking for.

For a TCXO oscillator: 40W normal (50W startup)

- 1) Maximum Current draw for 115VDC and 220VDC voltage sources.
- 2) **Maximum Power Consumption for 220VDC voltage source= 50 Watts**
- 3) **Heat Dissipation for 115VDC and 220VDC voltage sources= 50 Watts**
Watt = 1VRMS * 1A therefore Amp = Watt/VRMS
50 Watts/115VRMS = 0.43 A
50W/220V = 0.23 A

Desire for two DC inputs (instead of one AC and one DC input)

Option “SS OPT-DUAL-DC”

- Not currently released! (update 21 Aug 15 KW, Salesforce indicates this option is no longer available)
- Update to the FAQ below: Option “~~OPT-DUAL-DC~~” allows two DC inputs as long as they are both at the same voltage (both at 12 or both at 24/48)
- Refer to Salesforce: <https://na8.salesforce.com/01tC0000003uuoZ>

Q. Can the SecureSync be purchased with two DC inputs, instead of one AC and one DC input?

A. Email from Richard Fox, 8 Jan 2014) I discussed with engineering. We are not able to cost effectively design a dual DC unit for just 2 units. The non-recurring engineering costs will exceed the price of the units. Sorry. can they accept a unit with 1 AC and 1 DC power supply? See note above for an update to this answer (3 Nov 2014)

Issues with DC powered SecureSyncs not able to boot-up

A) Issues with power-up on DC voltages of about 46vdc or higher

1. 21-60VDC input units shipped prior to around Sept 2013 may have difficulty powering-up with input DC voltages above about 46vdc due to higher inrush current as the voltage goes up. The higher the voltage, the higher the inrush current.
2. If voltage is too high, SecureSync just sits there without ever powering up, unless the DC input voltage is reduced.
3. Refer to **ECN 3305** for circuit design changes to improve operation (“Improvement for 24/48V DC option high voltage startup”).

B) Issue with the external DC power supply not “beefy enough” to be able to supply enough current for inrush requirements

- SecureSync just sits there without ever powering up.
- Link to DC to DC converter data sheets (SynQor IQ12120QTC10NRS-G (10-17vdc) or SynQor IQ36120QTC10NRS-G (21-60vdc) : I:\Engineering\Engineering_Shared\Spectracom_Parts_ROHS\PS03R-xxxx-xxxx

“Secure locking device” (as stated in the user guide)

- The mating connector and cable clamp is included with the unit.
- Included in both the “DC only” and “AC/DC” Anc kits:

Mating connector and cable clamp Part Numbers:

A) Mating connector

- Amphenol P/N: DL3106A10SL-3S
- Our P/N: P240R-0032-002F (in Arena) at: https://app.bom.com/spec?item_id=1202844982&version_id=10221223528



B) Associated cable clamp/strain relief

Amphenol Cable clamp/Strain relief

- Amphenol P/N: 97-3057-1004(621)
- Our P/N: MP06R-0004-0001



This comment is referring to the available DC input power connector for the SecureSync. The AC input is a standard IEC line cord. The DC connector is threaded so that the mating connector can be physically and positively attached with a metal threaded nut. Though not necessarily recommended, the SecureSync could theoretically be picked up by its mating DC power connector without the plug falling off the back of the SecureSync and thereby causing the unit to lose input DC power.

Below are two pictures of the DC connector. It’s a little difficult to see from this picture, but the outer circle of the connector is threaded:

DC power only



DC and AC power



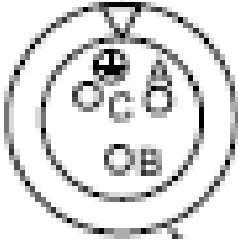
The DC mating connector is an “Amphenol” connector. Their Part Number is “DL3106A10SL-3S”. The Spectracom P/N is P240-0032-002F. The connector has solder cups for soldering wires to the connector pins.

Below is a better picture of both connectors together (the one on the back of the SecureSync is on the right and the mating connector is on the left). This picture shows the threads better than the above picture.

DC input Pinout/wiring info

SecureSync DC Connector: Amphenol P/N DL3102A10SL-3P

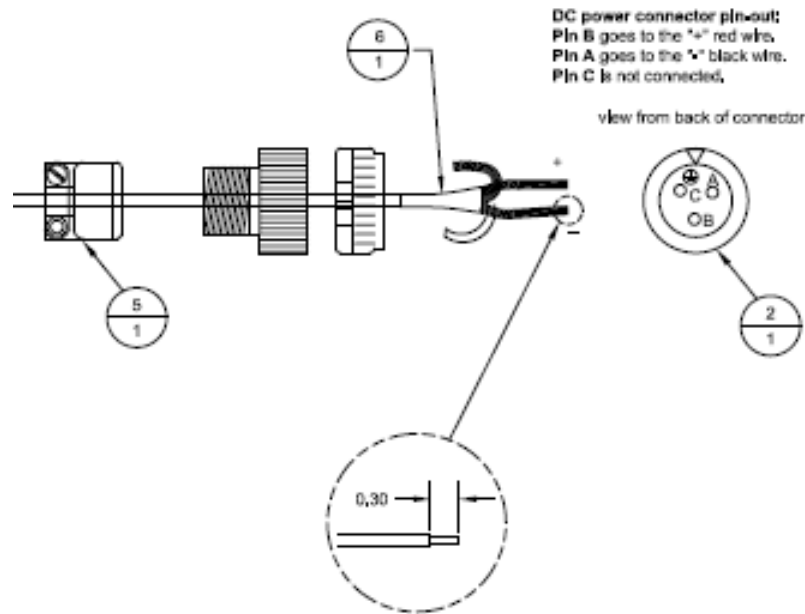
Mating DC Connector: Amphenol P/N DL3106A10SL-3S



Pin B goes to the most positive DC voltage of the DC source. For +12V or +24/48V this would be the positive output from the DC source. For a -12V or -24/48V DC source this would be the ground or return of the DC source.

Pin A goes to the most negative voltage of the DC source. For +12V or +24/48V this would be the ground or return output from the DC source. For a -12V or -24/48V DC source this would be the negative output from the DC source.

Pin C goes to the Earth ground of the DC source.



DC power wiring

- A cable of 6 feet or less, using 16AWG wire, with adequate insulation for the DC voltage source should be used with this connector.
- The 6 feet or less cable is due to inrush current causing voltage drop. Refer to email below.

Specific to 24/48vdc input

Email from Sam Otto: I checked with design engineer ([Mark McGregor](#)) who recommends a 24VDC, 6.25 Amp, 150 watt power supply using 16 gauge wire less than 1 meter from out unit. The reason for this is the inrush current causes the voltage to drop which results in an under voltage lockout preventing your SecureSync from powering on.

Pin B goes to the most positive DC voltage of the DC source. For +12V or +24/48V this would be the positive output from the DC source. For a -12V or -24/48V DC source this would be the ground or return of the DC source.

Pin A goes to the most negative voltage of the DC source. For +12V or +24/48V this would be the ground or return output from the DC source. For a -12V or -24/48V DC source this would be the negative output from the DC source.

Pin C goes to the Earth ground of the DC source.

Important! SecureSync is earth grounded through the DC power connector. Ensure that the SecureSync is connected to a DC power source that is connected to earth ground via the grounding pin C of the SecureSync DC power plug supplied in the ancillary kit.

Leakage current (current leakage)

➤ Refer to Salesforce case 163902

Leakage current is the **current** that flows from either AC or DC circuit in an equipment to the chassis, or to the ground, and can be either from the input or the output. If the equipment is not properly grounded, the **current** flows through other paths such as the human body.

**** (PS06R-2Z1M-DT01) Available AC to 24VDC converter for Dual AC input power**



Shortcut to MFG data sheet (SL Power MENT1220.pdf): <I:\Engineering\Engineering Shared\Spectracom Parts ROHS\PS06R-xxxx-xxxx> (Note: we use power option 2)

Shortcut to price info in Salesforce (“SecureSync Dual AC Power Option”)

<https://na28.salesforce.com/01tC00000039TX8?srPos=0&srKp=01t>

Description from Salesforce: SecureSync Dual AC Power Option. This feature provides a second AC power input to the system. NOTE: This option can only be ordered with SecureSync units with 24 VDC power input option, i.e., Model Numbers 1200-2XX.

Chassis/Power Configuration needed to use a PS06R-2Z1M-DT01 (dual AC input)

- **SecureSyncs:** 24-48vdc input (not 12vdc)
- **9483s:** Add **Option 15** (24-48vdc input)
 - Appears PS06R-2Z1M-DT01 is not inherently included with Option 15
 - Appears its available for separate purchase to be included with Option 15,

Specs

Specifications		
Output Specifications		
Line Voltage Regulation	Including Cord	2%
Load Voltage Regulation	Including Cord	5%
Ripple	1% Vp-p of Vnorm, max.	
Transient Response	5 msec from 25% to 75% load change typ., < +/-5% Over/Undershoot	
Turn on Delay	Less than 3s over entire input range	
Turn on Overshoot	Less than +/-5% of Vnorm. over entire input range	
Over Temperature Protection	Active	
Over Current Protection	Higher than 120% of Inorm. Cyclic Mode	
Short Circuit Protection	Cyclic Mode	
Temp. Coefficient	±0.05% / °C	
Protection Mode	Auto Recovery OCP, SCP Latch protection OTP, OVP	
Input Specifications		
Voltage	100-240VAC -10%, +10%	
Line Frequency	47-63Hz	
Input Current	2.0A max. @ 90VAC	
Protection	Internal primary current fuse	
Power Factor Correction	Complies with EN61000-3-2 class D	
Environmental Specifications		
Thermal Performance	Operating Temperature	0° C to 40° C with no Derating
Cooling	Convectional	Non-ventilated Enclosure
Relative Humidity	Non-condensing	5% to 95%
Altitude	0-10,000 feet	
Storage Temp	-20° C to +85° C	

- **Input:** 100-240VAC, 57-63 Hz, single phase **Input current:** 4A max
- **Output:** 24vdc, 9A
- **Temp range** -20C to 70 C.
- The **size** of the power adaptor
 - **Width** 4 ¼ Inches or 10.795 Centimeters
 - **Length** 8 1/8 Inches or 20.6375 Centimeters
 - **Height** 2 Inches or 5.08 Centimeters
- P/N of the finished adaptor is **PS06R-2Z1M-DT01** (in finished goods)

- **MFG / MFG P/N for this transformer:** SL Power P/N: MENT1220A2451F01
- This is a **PS06R-2Z1M-DT02** (kept in the stockroom) that is modified for the SecureSync's/ 9483s DC input connector. This part is shipped to us with a 6 pin output connector, that we remove here and install our connector before shipping it to customer

Link to drawing (PS06R-2Z1M-DT01) showing how to modify the raw adapter (in Arena):
https://app.bom.com/items/detail-spec?item_id=1202845989&version_id=10257862298

PS06R-2Z1M-DT01/B - PS06R-2Z1M-DT01 - PWR SUP ASSY,SW,10	1.0000 - AKAT00060
10 FASSY -	
10 E01003 - 3/16in SLEEVE SHRINK, BLACK	1.0000 Qty Reqd
20 MP02-0003-0001 - LABEL,POLYESTER,SILVER,2.0X.75in	1.0000 Qty Reqd
30 MP06R-0004-0001 - CABLE CLAMP,CIRC,10SL/12S,BLK ZINC	1.0000 Qty Reqd
40 P240R-0032-002F - PLUG,CIR,3P,F,FMLB,SOLDER,16AWG,13	1.0000 Qty Reqd
50 PS06R-2Z1M-DT02 - PWR SUPP,SW,100-240VAC,24VDC,9A,-:	1.0000 Qty Reqd
60 PS06R-2Z1M-DT01-PD - PWR SUP ASSY,SW,100-240VAC,24V	0.0000 Qty Reqd
20 TEST -	

- This power supply is Energy Star 2.0 Level V compliant,
- This power supply meets EISA 2007 and will operate to -20C, even though it is not specified on the product data sheet
- The SecureSync/9483 Ancillary kit will still include the raw parts for the DC connector, but they won't be needed if they purchase this available converter from us.

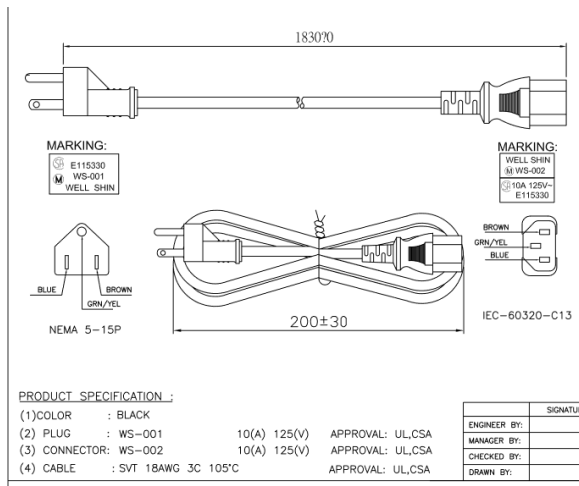
AC input

- Converter has standard IEC320 **C14** grounded connector for AC input.

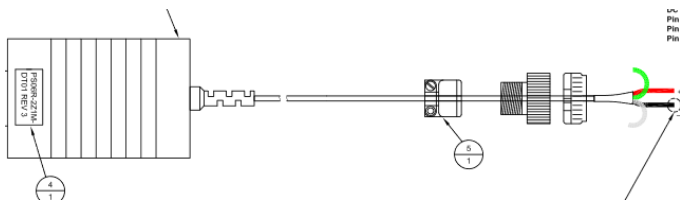


Provided AC Line cord (CA06R-1513-0001)

- Refer also to "**AC power cable included in ancillary kit**" (in this same document)
[CA06R-1513-0001](#) AC CORD,5-15P to **C13**,18AWG,10A,125V,105C
- The cable length of the 2nd AC power is 3 ft. or 0.9 Meters



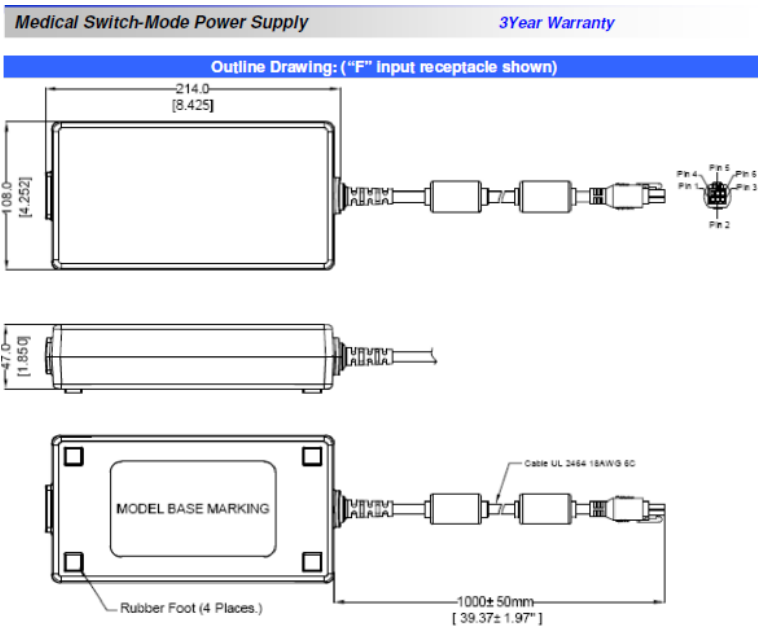
DC Output



- Length of cable ~38 inches
- **DC Connector** Our P/N P240R-0032-002F (Amphenol Pre-Earth/FMLB threaded connector DL3106A10SL-3S, for mating with the input DC connector on the back of the chassis)

Mechanical mounting for the power supply

- No mounting is provided- any mounting needs to be custom
- Manufacturer's Data Sheet contains a mechanical drawing that can be provided as a reference for a customer to create some type of custom mount:



****Humidity/Power/BTU specs (Heat dissipation)**

Humidity: 10% - 95% relative humidity, non-condensing @ 40 C

Power Draw (SecureSync and NetClock Model 9400s)/ Heat dissipation (BTU/hr)

- TCXO: 40W normal (40W start-up) 136.48566532 BTU/hr
- OCXO: 40W normal (50W start-up) 136.48566532 BTU/hr normal (170.60708165 BTU/hr startup)
- Rb: 50W normal (80W start-up) 170.60708165 BTU/hr normal (272.97133064 BTU/hr startup)

BTU disbursement rating/ Heat dissipation

Email from Tom Richardson

A BTU (British Thermal Unit) is the amount of heat necessary to raise one pound of water by 1 degree Fahrenheit (F).
1 Watt is the power from a current of 1 Ampere flowing through 1 Volt.

1 kWh = 3413 BTU

Using how many Watts the unit takes to warm up and neglecting the hours part, 50 Watthours = 171 BTU, 80 Watthours = 273 BTU

This is sort of like apples and applesauce because BTUs are usually used in cooling and Watts are energy. Customer probably really wants to know how many BTUs it takes to cool a unit.

Email from Scott Holmes

Tom's explanation is a good one.

Just a few definitions that might help.

Power is the rate energy is consumed and can be expressed in watts, kilowatts, etc.

Energy is the amount of power consumed, expressed in watt-hours, kilowatt-hours, BTU, etc.

So, as Tom says it's apples to applesauce. The watt is an SI unit of power and the BTU an Imperial unit of energy.

Just to add to Tom's 1kWh = 3413 BTU, you can also say 1W = 3.41 Btu/hr, if this makes it a bit clearer.

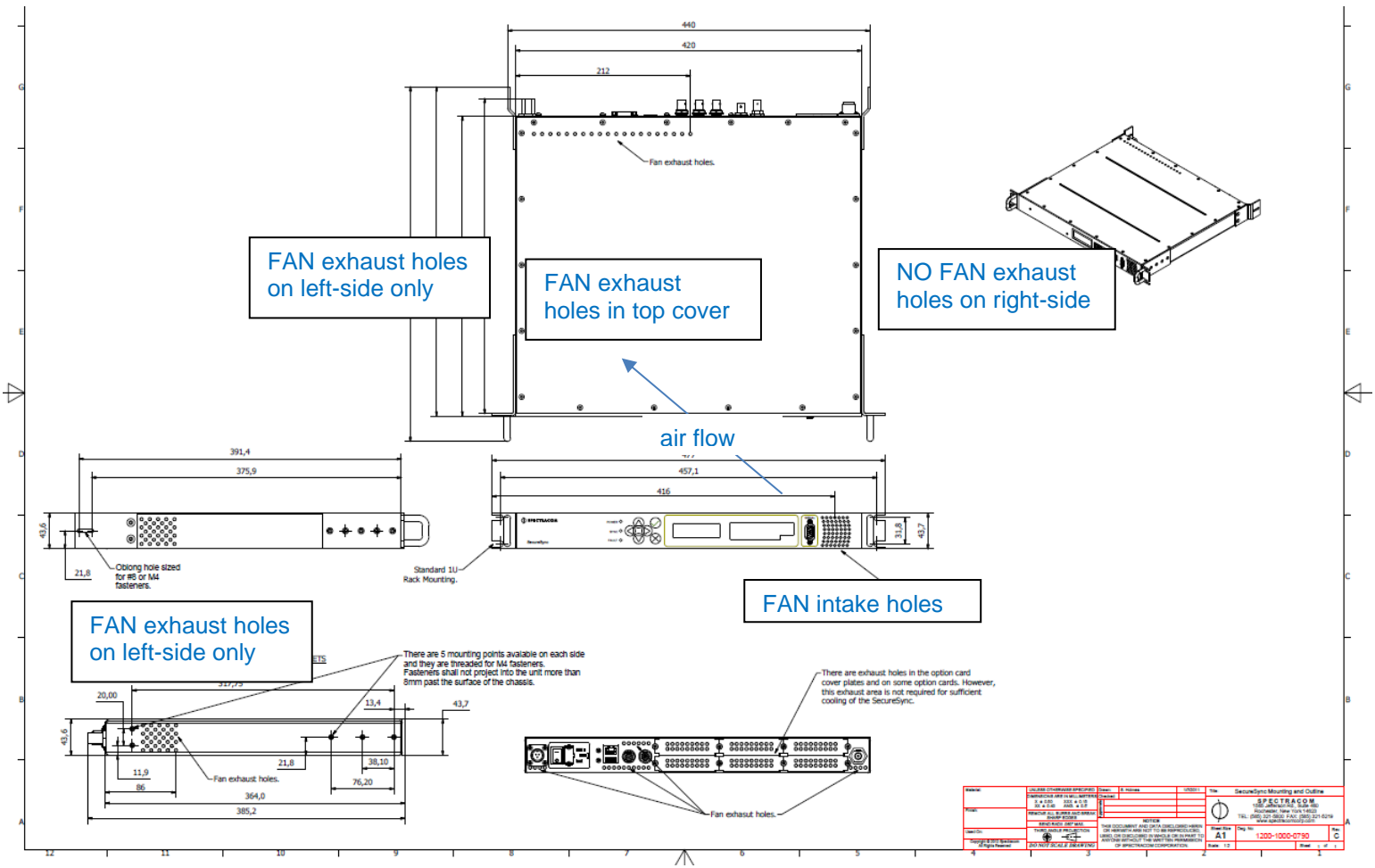
Email from Mark McGregor:

There should be two BTU ratings. The ones Tom gave (above) are for while the OCXO and Rb units are warming up. If you have the unit running for more than 30 minutes, the rating will drop a bit to the 40W max for OCXO and 50W max for Rb. If they are using it for cooling fan rating, I would just give them the warm up power numbers, as it will have them choose a larger fan.

** Airflow requirements/Cooling fan/ Temperatures

Airflow thru chassis/Airflow requirements

- Drawing below (1200-1000-0790rd) at [I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\CAD - 3D drawings\SecureSync with Trimble or No GPS receiver\1200-1000-0790rd \(mtg and outline\).pdf](I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\CAD - 3D drawings\SecureSync with Trimble or No GPS receiver\1200-1000-0790rd (mtg and outline).pdf)



Rack mounting requirements:

- Refer to online SecureSync user guide (except below) at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/Mounting.htm
- The maximum ambient operating temperature must be observed. See [Mechanical and Environmental Specifications](#) for the operating temperature range specified for the type of oscillator installed in your SecureSync unit.
- If the SecureSync unit is to be installed in a closed rack, or a rack with large amounts of other equipment, a rack cooling fan or fans should be part of the rack mount installation.
- Installation of the unit in a rack should be such that the **amount of air flow** required for safe operation of the equipment is not compromised.

SecureSync Chassis Cooling/Airflow requirements

- Refer to <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Cooling-Temperature testing>

AirFlow rate: Refer to Salesforce Case 224578, and docs in link directly above

The cooling fan, while running (it is always temperature controlled in early Serial Numbers, newer units can be temp controlled or always spinning), pulls ambient air in through the right side of the front panel. The chassis was intentionally designed to have holes only on the back of the left-side of the chassis, so air is essentially “ducted” to and across the back end of the chassis for cooling (drawing heat away from the components located towards the front of the chassis).

Slightly modified email from Dave Sohn (7 Nov 2018) SecureSync has a single fan on the front of the unit (right side as you look at it). Airflow is designed from front to rear. There is venting in the rear, left-side rear, and top-left rear. The side and top vent holes are not required to be clear for correct temperature control.

1. The fan is rated for 7 cfm
2. The intake is in the front and exhaust holes are located in the rear panel, back of top cover and sides of the chassis
3. The exhaust holes in the top cover and sides can be blocked without affecting cooling
4. There should be at least ½” of air space at the intake and rear exhaust
5. The unit is designed for airflow from Front to Back to maintain proper ventilation within the operational temperature range
6. The fan should be operating when the unit is powered (Always On).

FAQs about cooling/airflow requirements

Q (Per Salesforce Case 224578) Is there a predicted pressure curve with respect to airflow on a SecureSync cooling fan? Customer is trying to capture the flow resistance through the module. He also asked if we have any thermal shock data for this unit (°C/min).

A

Q (Per Salesforce Case 238680) We are attempting to utilize the Securesync 1200 in a 19" electronics rack and I was hoping you could provide some information. 1) Does the Securesync 1200 have any mounting provisions on the side for mounting slides? (for a 19" electronics rack) 2) Do you have a mechanical drawing showing the overall size and the size/location of any mounting provisions? 3) Do you have a 3D CAD model (STP file) you could send? This would aid us in integrating into our electronics rack.

Q (Follow-up question from Salesforce Case 238680) I'm looking back over the model and drawings you sent me. Are the side vents only for one side of the unit?

Keith's response: Yes. Left-side only (as looking at the front panel). This ducts the incoming air from the front-right side to the rear-left side.

There are no mounting provisions on the top or bottom either, correct?

Keith's response: Correct.

The only mounting holes are for the front and rear brackets, correct?

Keith's response: Correct.

How much air flow is required for safe operation of the equipment based on the below?

Keith's response: 7 cfm (the rating of the cooling fan)

- If the SecureSync unit is to be installed in a closed rack, or a rack with large amounts of other equipment, a rack cooling fan or fans should be part of the rack mount installation.
- Installation of the unit in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Q (per Salesforce Case 241188) Have some additional information from our Mechanical Design team. They stated that there is 0.7 inches of clearance between the side of the Unit and the side of the installation shelf... effectively creating a 0.7" wide plenum to remove/draw the heat.

Can you confirm whether that amount of clearance from the output vent of the unit is sufficient or specify the minimum amount of clearance required from these vents? Are the vents on the side, but towards the rear of the unit? Can your team provide mechanical drawings to show where the output vents are located?

A Per Keith (4 Aug 2020) This was a question about AMDR unit, sent over to OGS I to respond

A Reply from Alex Payne (4 Aug 2020) I am confirming the following information for the SecureSync:

- 1) The fan is rated for 7 cfm;
- 2) The intake is in the front and exhaust holes are located in the rear panel, back of top cover and sides of the chassis;
- 3) The exhaust holes in the top cover and sides can be blocked without affecting cooling,
- 4) There should be at least 1/2" of air space at the intake and rear exhaust,
- 5) The unit is designed for airflow from Front to Back to maintain proper ventilation within the operational temperature range;
- 6) The fan should be operating when the unit is powered (Always On).

Cooling fan (not applicable to Model 9489)

- Our P/N for the cooling fan: B351R-06R5-000H (in Arena) https://app.bom.com/items/detail-spec?item_id=1202835021&version_id=10221213508&orb_msg_single_search_p=1&redirect_segno=7755752740
 - **Mfg:** Sunon Fans
 - **MFG P/N:**
 - **Newer P/N** (as of August 2020, not sure when it changed): MF35100V1-1000U-A99
 - **Original P/N:** GM0535PFV1-8.GN

Qualified alternative fan from different manufacturer (same specs): MULTICOMP P/N MC36314



Life expectancy of the fan, from Mfg. Data sheet): 60000 hrs @ 40°C (about 7 years of continuously on)

Detailed info about the cooling fan:

- Refer to the online SecureSync user guide at: <http://manuals.spectracom.com/SS/Content/NC> and [SS/Com/Topics/OPRTN/TempMon.htm](http://manuals.spectracom.com/SS/Com/Topics/OPRTN/TempMon.htm)
- Refer to <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Cooling-Temperature testing>

Fan voltage: 5vdc

AirFlow rate: **7CFM** (refer to Salesforce Case 224578, and docs in link directly above)

- **Newer P/N** (as of August 2020, not sure when it changed): **MF35100V1-1000U-A99: 7.2 CFM**
- **Original P/N:** **GM0535PFV1-8.GN: 7 CFM**

Acoustic Noise of the cooling fan:

- Requested on Case 283536 (April 2022)

General info: Refer to <https://www.sunonusa.com/technology/low-noise-design/>

- **Newer P/N** (as of August 2020, not sure when it changed): **MF35100V1-1000U-A99:**

Below info from:

[https://www.sunon.com/eu/MANAGE/Docs/PRODUCT/299/367/SUNON%20DC%20Brushless%20Fan%20%20Blower\(255-E\).pdf](https://www.sunon.com/eu/MANAGE/Docs/PRODUCT/299/367/SUNON%20DC%20Brushless%20Fan%20%20Blower(255-E).pdf)

■ Specification

	Bearing	Rated Voltage	Power Current	Power Consumption	Speed	Airflow	Static Pressure	Noise	Weight	Curve
	VAPO	(VDC)	(mA)	(WATTS)	(RPM)	(CFM)	(inch-H ₂ O)	(dBA)	(g)	
MF35100V1-1000U-A99	●	5	135	0.68	10000	7.2	0.22	28.0	10.5	1

- **Original P/N:** **GM0535PFV1-8.GN:**

Below info from: <https://datasheet.octopart.com/GM0535PFV1-8.GN-Sunon-Fans-datasheet-1803.pdf>

Model	P/N	Bearing	Rating Voltage	Power Current	Power Consumption	Speed	Air Flow	Static Pressure	Noise	Weight
		VAPO	(VDC)	(AMP)	(WATTS)	(RPM)	(CFM)	(inch-H ₂ O)	(dBA)	(g)
GM0535PFV1-8	GN	●	5	0.15	0.8	9500	7.0	0.18	28	10.5

SecureSync Chassis Cooling: The cooling fan, while running (it is temperature controlled), pulls ambient air in through the right side of the front panel. The chassis was intentionally designed to have holes only on the back of the left-side of the chassis, so air is essentially “ducted” to and across the back end of the chassis for cooling (drawing heat away from the components located towards the front of the chassis).

Per Dave Sohn (7 Nov 2018) SecureSync has a single fan on the front of the unit (right side as you look at it). Airflow is designed from front to rear. There is venting in the rear, side rear, and top rear. The side and top vent holes are not required to be clear for correct temperature control.

Storage Temperature: -40° to 85°C storage range

Indications of the fan operation/fan has failed

Q. If the fan is left in the ‘always on’ function what is the expected time before it may stop working and will the SecureSync indicate a failure of the fan in anything other than the logs?

A **Keith’s response (10 Feb 16):** the life expectancy for the fan when always running is 60000 hrs @ 40°C (about 7 years). As there is no feedback from the fan indicating whether or not it’s actually spinning, there isn’t a direct indication of the fan’s operation (log entries, alarms or alerts) available for the SecureSync.

However, software version 5.3.1 also added SNMP traps and gets and Minor/Major alarms associated with the internal temperature. If the cooling fan was to fail and this resulted in the internal temperature exceeding a user-specified threshold, a Minor and/or Major alarm can be optionally asserted and an optional SNMP trap can be sent to an SNMP Manager. Alarms and SNMP Trap alerts for high/low temperatures are configured in the **Management -> Notifications** page of the browser (with version 5.3.1 or above installed), System tab (as shown below)



checkboxes in this tab allow the associated temperature traps to be enabled to be sent, and the user-configurable temperature thresholds are configured in the fields towards the bottom of this tab. “Readings above threshold” allows a delay (in seconds) between each insertion of this alarm (for instance, set it to “5” for a 5 second delay between each insertion of the condition, if the temperature remains above the specified value for a length of time. this prevents it from being continuously inserted as the temp remains above the threshold).

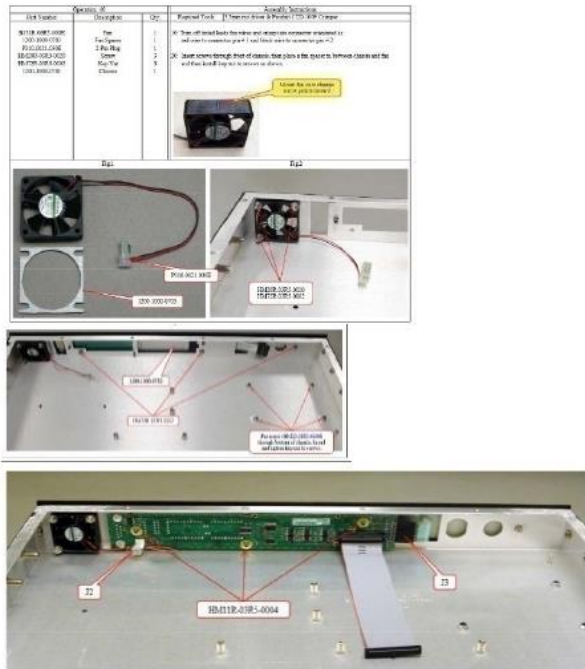
Replacing the cooling fan in the field

➤ Refer to Salesforce case 159470

Email from Dave L (18 Apr 18) It is not impossible to replace the fan, just not really easy. You would need to disassemble the front panel a bit to prevent the fan screws from turning if they will not loosen or tighten. If they are manageable you would not need to remove the front panel.

Here are a few photos of the product. Please have a look and see if this is something you would want to tackle or if you would like to RMA the Securesync. I can send you a fan with the connector already installed.

Here is a view of the inside showing the screw locations, this should help.



Environment Operating (Disc) Temperature:

- **-20°C to 65°C** operating range with the two **OCXO** variants (Standard and high performance)
- **-20°C to 55°C** operating range with the **Rubidium** oscillator (KW Note: as of 11/11/2011, this upper-end spec changed some time ago. It used to be only +50°C, instead. Per the note further below, it appears this change occurred in Aug, 2010).

Excerpt below from page 3, SecureSync datasheet (July 2020)

Environmental

	Operating	Storage	MIL-STD-810F
Temperature	-20 to +65°C (+55°C for Rb)	-40 to +85°C	
Humidity	0%-95% RH non-condensing @ Δ0°C		

Operating temperature spec change (due to UL requirements)

Email from Tony Diflorio to Hughes network (1/13/12)

This temperature spec was first changed in August 2010 – see attached datasheet from Aug 17, 2010 (rev F). Which is well before HNS selected Spectracom for the Jupiter project. Also, our engineers have informed me that the unit will operate at +70C, however, due to UL certification requirements the metal surfaces in the unit are not allowed to get above +70C and thus the reason for the change.

Q. Also can you provide information about what can be expected if the units are run beyond these limits? We do not intend to run them outside the range but we need to know the impact to the performance if the units are run beyond the limits.

A (Email from Dave Sohn) Initially as the unit is heated above the temperature specification, the oscillator driving the timing system will become unstable. This instability will affect our timing performance and all output performance. As the unit continues to be heated, the unit will become unstable and unresponsive. On the low end, the first failure will be the front panel display failing to operate, and then the remainder of the unit will become unstable and unresponsive.

Fan Control mod / operating temperature/hysteresis (not applicable to Model 9489)

- Requires both and software versions 5.3.1 or above, and a hardware mod in earlier units
- Software version 5.3.1 and above (and only if EEPROM has either been reprogrammed or programmed at factory (starting ~Dec 2015) for fan control. **Approximate** cut-in S/N **11106** (which shipped 7 Jan 2016)

- All new units with Front panel PCB Rev 5, or above (~Dec 2015), installed have the necessary mods.
- Some earlier units shipped before front Panel PCB Rev 5 was incorporated, had the mods performed to add necessary changes.

A) Necessary Hardware mod

- 1) Reprogram EEPROM
- 2) Changes to Front Panel Assy (1200-1000-0300): R8, R32 and Q1 (changes implemented in PCB Rev 5., 1200-0000-F005 5 Dec 2015)

ECO-000665.Change R8 from DNP to R116R-6491-YF0B,6.49k resistor. Change R32 from R116R-0000-YJ0B to R116R-1002-YF0B, 10k resistor. Change Q1 from Q030R-7002-010R to Q030R-2302-000V.	Nov 16, 2015
---	--------------

B) Software update to 5.3.1 or above

- Software version 5.3.1 and above (and only if EEPROM has either been reprogrammed or programmed at factory (starting ~Dec 2015) for fan control.
- Refer to **ECO-665** (completed 12/07/2015) in Arena: https://app.bom.com/changes/detail-summary?change_id=2385461508
 - New software to allow for control of fan (v5.3.1)
 - Added new EEPROM configuration change for SecureSync and NetClock 9483's units which indicate Front Panel Modification is present and software can control the Fan.
 - Ability to configure Major/Minor Alarms on temperature causing System and Alarm log logging and the sending of SNMP Traps and Emails on exceeding user defined temperature levels.
 - Ability to configure Fan Always ON, or User defined Fan on/off Temperature levels.

How to tell if the EEPROM has been programmed/reprogrammed for fan control:

- 1) There will be a gear ICON next to “**System Status**” (on the left side of the **Home** and **System Monitor** pages of the browser) if it’s programmed for software fan control.



There won't be an ICON next to System Status if the EEPROM hasn't been reprogrammed/programmed since ~Dec 2015). Approximate cut-in S/N **11106**, which shipped 7 Jan 2016)

- 2) Upon each boot-up, the Fan Control feature detection is logged in the System log.
 - Log entry asserted after each boot-up (starting in v5.3.1) with mod installed: **Temperature Monitor daemon has started (TEMPD)**

(except Model 9489s, which don't have a cooling fan) Software version 5.3.1 added fan control to software, based on temperature (ETX temp)

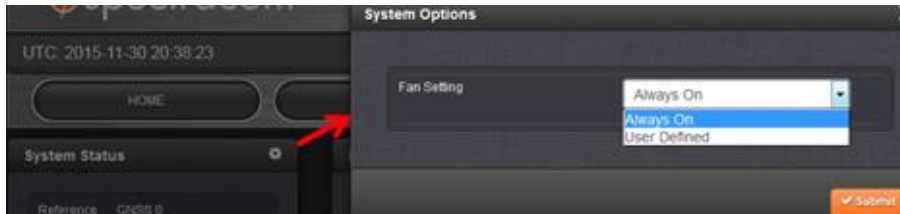
Refer to online securesync manual:

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

Note the EEPROM needs to be reprogrammed to move fan control to software (not just update the software to v5.3.1)

- If the EEPROM has been reprogrammed, select the **gear** ICON next to “**System Status**” in the upper-left corner of the **Home** page (or the Gear ICON in the **Tools -> System Monitor** page). The pop-up window allows selection of fan “**Always On**” or “**User Defined**”. Selecting “User Defined” allows selection of fan turn-on temp (40c by default) and fan off temp (30c by default).

- **Home** page



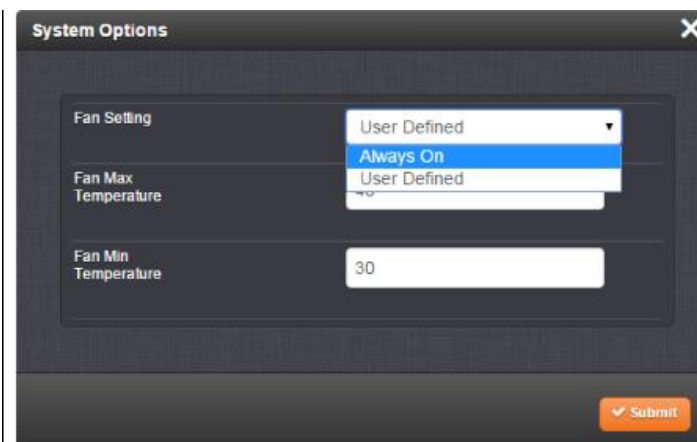
OR

- **Tools -> System Monitor** page



After selecting “**User Defined**”, fan turn on/turn off temps are then displayed underneath (Based on CPU temp):

- **User Defined:**



A user determines the:

- **Fan Max Temperature:** The CPU temperature in °C at which the fan will turn ON. It is advisable to set this temperature no higher than 40°C.
- **Fan Min Temperature:** The CPU temperature in °C at which the fan will turn OFF (the default is 30°C).

If the EEPROM has not been reprogrammed and the software is updated to v5.3.1, the fan is still controlled by sensor on the front panel (not controlled by software).

Q. It is stated you need the SecureSync to be “equipped with Front Panel Fan Modification”. How do you know if a unit has this modification or is this something that is in all units with the front fan?

A. **Keith’s response (10 Feb 16):** The quickest/easiest way to tell if this hardware modification is installed (without even looking at the SecureSync) is if the SecureSync was purchased/received before December, 2015, and if it has not been returned to the factory for service since this same time-frame, it won’t have this modification installed.

Specific to the SecureSync itself, to tell if the modification has been installed and with version 5.3.1 or above software installed- login to the Home page SecureSync’s web browser. If this modification has been installed, there will be a gear ICON next to “**System Status**” (left side of the Home page) as shown below (the gear ICON opens a pop-up window to configure the cooling fan).



If the modification is not installed (all units shipped prior to ~Dec 2015 and have not yet returned for service since the Dec 2015 time-frame) there is no gear ICON to the right of “System Status”. Note this mod for the cooling fan to also be controlled by the ETX module (CPU) as well as the front panel sensor can be added to earlier units as a warranty modification at the factory.

Q Is the fan only manageable using the new web interface or is there a place in the older web interface and the command line interface to manage this new feature?

A **Keith’s response (10 Feb 16):** The fan control and temperature alert functionality is only manageable via the newer (black/charcoal) web browser. It is not available via the classic interface browser or via the CLI interface.

Q With units having the fans constantly running, if the fan fails is it covered in general for RMA and if so is there a time limit for this kind of RMA repair?

A **Keith’s response (10 Feb 16):** The SecureSync, including the cooling fan (whether or not the fan is constantly running) has a 5 year warranty from the date of purchase. If a fan was to fail prior to the end of this warranty period, it would be covered under warranty. After 5 years, the fan would no longer be covered under warranty.

Adding fan control mod to units while they remain “in the field”

- Refer to EEPROM patch (Thierno verbally confirmed this patch works)
 - ICS-Eng/Projects/Lafayette/200 Engineering Documents/Working Files/EEPROM/[patch_img.bin](#)
- Refer to Cases such as 180394 (info from this case is below)

Q I have been discussing upgrade SecureSync units to add fan control, and understand that two steps are necessary:

- Replace the front panel board assembly
- Replace the CF card with pre-loaded 5.8.2 code (downgrade is NOT recommended)

A **Reply from Dave L (30 Nov 18)** Actually, there are three steps necessary to update the fan controls on the SecureSync. This third step involves reprogramming an EPROM to tell the system the new fan control hardware has been added. Without the EPROM change, the software controls for the fan will not be enabled.

The EPROM cannot be reprogrammed in the field by the user. It must be done at the factory. I am asking our engineering group if there is any other way you could do this in the field. Please standby while I await the answer. If this is possible we will get you a cost for the front panel boards.

Alarms/SNMP traps/email alerts for high temperatures (versions 5.3.1 and above)

High Temperature alarm/alerts

- Refer to online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm
- Version 5.3.1 also added SNMP alerts for high temperatures (*Management* -> *Notifications* page, **System** tab)
- The default temperature threshold value for both Minor, and Major Alarms is **100°C**

The screenshot displays the configuration interface for high temperature alarms. It features four rows of alarm settings, each with a checked checkbox and a text input field. Below these are two sections for 'Minor Alarm Threshold' and 'Major Alarm Threshold', each containing 'Minimum Temperature (C)' and 'Readings above Threshold' input fields. The values '100' and '1' are entered in the respective fields. Red circles highlight the alarm settings and the threshold sections.

The alarms are similar in behavior to the GPS Number of Satellite Major and Minor alarms. In this case the user can set a Minimum Temperature Threshold value for both the Major and Minor alarms. The user can also set a number of times the value above the threshold must be present before asserting the Major or Minor Alarm. A value of 1 means that the value was read once, a minute passed and on reading the value again, the temperature exceeded the threshold. The number of reads is user settable to allow for environmental conditions where more than 1 read is required to validate accurate temperature. Increasing the value requires N multiple consecutive reads of temperature above the minimum threshold before asserting the alarm.

Environmental temperature specs in datasheet

- These are the operating temperature specs for the ambient air temperatures **outside** SecureSync
- We do not provide specs in datasheet for **internal** temperatures

	Operating	Storage	MIL-STD-810F
Temperature	-20 to +65°C (+55°C for Rb)	-40 to +85°C	

Recommended temperature settings for user-defined high temp alerts (per Ron Dries)

- We recommend **Minor** alarm at **90 deg C**
- We recommend **Major** alarm at **100 deg C**

Q ...in Securesync there are three temperature value which are CPU, board and oscillator. I would like to know what is the threshold or max operational temp level. For the temp alarm monitoring the default value is 100°C and it is referring to what. CPU, board or oscillator ? What is the recommended value for temp. setting?

A . Reply from Jodi (30 Mar 17) Please see the below excerpt from the SecureSync online user manual:
The default temperature threshold value for both Minor, and Major Alarms is 100°C. With simultaneous alarm triggerings, the Major Alarm will override the Minor Alarm, i.e. you will be notified only about the Major Alarm. If you want to be notified early about a rise in temperature, a recommended setting for the Minor Alarm temperature would be 90°C. Please note that it is not advisable to set the Major Alarm temperature to a value higher than 100°C.

We do not have a range of recommended temperature for the unit, but we do have a recommendation of NOT exceeding 90 degrees C

Storage of the temperature monitor settings (configs)

- These settings are stored in the `/home/spectracom/config` folder - `temp.conf` file

```

1 MINOR 100000 1
2 MAJOR 100000 1
3 SETTING 0
4 MINTEMP 30000
5 MAXTEMP 40000
6

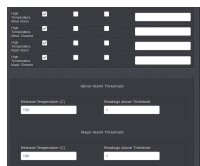
```

Q. If the fan is left in the always on function what is the expected time before it may stop working and will the SecureSync indicate a failure of the fan in anything other than the logs?

A. Keith's response (10 Feb 16) : the life expectancy for the fan when always running is 60000 hrs @ 40°C (about 7 years). As there is no feedback from the fan indicating whether or not it's actually spinning, there isn't a direct indication of the fan's operation (log entries, alarms or alerts) available for the SecureSync.

However, software version 5.3.1 also added SNMP traps and gets and Minor/Major alarms associated with the internal temperature. If the cooling fan was to fail and this resulted in the internal temperature exceeding a user-specified threshold, a Minor and/or Major alarm can be optionally asserted and an optional SNMP trap can be sent to an SNMP Manager.

Alarms and SNMP Trap alerts for high/low temperatures are configured in the **Management -> Notifications** page of the browser (with version 5.3.1 or above installed), **System** tab (as shown below)



Checkboxes in this tab allow the associated temperature traps to be enabled to be sent, and the user-configurable temperature thresholds are configured in the fields towards the bottom of this tab. "Readings above threshold" allows a delay (in seconds) between each insertion of this alarm (for instance, set it to "5" for a 5 second delay between each insertion of the condition, if the temperature remains above the specified value for a length of time. this prevents it from being continuously inserted as the temp remains above the threshold).

Software versions 5.3.0 and below

- All original as well as all units shipped Oct 2014 until 5.3.1 was released (~Dec 2015) hardware caused cooling fan to turn on at 40C.
- Units shipped between ~Feb 2014 and ~Oct 2014: Hardware (resistor change) caused the cooling fan to turn on at 50C (instead of 40C).
- Until version 5.3.1 was cut-in to manufacturing (~Dec 2015) Temperature reading for the cooling fan operation was

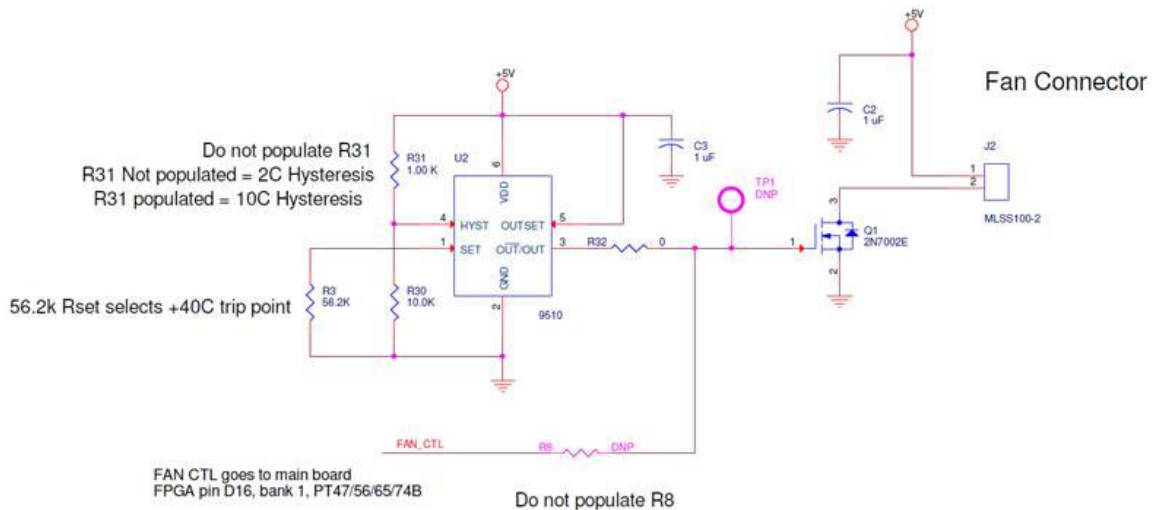
based on a temperature sensor located on the front panel assembly of all units. As of at least Dec 2015, this sensor's temperature reading is NOT reported anywhere (it's not one of the three temperatures reported in the browser with later software versions, for example). It just turned the fan on and off (version 5.3.1 with an EEPROM change incorporated moved fan control to software, based on CPU temp or fan always running).

Hysteresis

- Used to turn the fan off, once it's on.
- The Temperature must drop by the set Hysteresis value to off, once it is on, in order for fan to turn off.
 - **Example:** If Hysteresis is set to 10C, the temperature must drop by 10C from what it was when the fan turned on, before the fan turns off again.

Email from Mark McGregor (12 Oct 2015) There was a period of time when the SecureSync fan control located on the front panel was changed from its original settings of fan turn on at 40C and 10C Hysteresis (for hysteresis, temperature must drop 10C to turn fan off once it is on). This will be present only on the newer front panels with bare PCB 1200-1000-0300 Rev. C. The 1200-1000-0300 Rev. C have an SMT connector to the front panel overlay, J3, rather than a through hole connector.

The 50C turn on, 2C hysteresis was done by making front panel resistor R3 to 48.7k and new resistor R31 not populated, DNP.



When the Harris high RB failure rate investigation was done, it was discovered that the change to have the fan run less was not good for Rb units and later for the ETX as well.

So, some time last year, the newer front panels fan control has been changed to be back to the original 40C turn on, with 10C hysteresis to try to keep the RB and ETX as cool as possible.

The original 40C turn on, 10C hysteresis was restored by making front panel resistor R3 back to the original 56.2k and new resistor R31 populated, R116R-1001-YF0b, 1k-ohm.

Note (3 Feb 2014 KW) Per Mark McGregor - ECN 3381 is changing the temp for fan operation. Added changes to decrease fan switch temperature delta for on to off from **10C to 2C**. Also changed fan turn on temperature from 40C to 50C. This was to minimize the frequency shift of the oscillator getting pushed around when the fan cycles and drives the temperature inside the box from 45C to 35C faster than the control loop can follow.

Summary of changes to the control of the cooling fan (such as turn-on/turn-off temps)

- **Version 5.3.1** (Enhanced Fan Control) since ~ Dec 2015.
 1. Now “software” controlled (instead of using the sensor on the front panel), **if** the front panel fan Modification is performed (removes control from the front panel sensor to software control based on ETX temperature).

2. Factory default setting is fan always on.
 3. If the software is updated to version 5.3.1 and the hardware mod is not installed, the fan continues to operate as it did before the software was updated to version 5.3.1 (the front panel sensor still controls the fan).
 4. With a hardware change to the front panel assembly an “or” switch is added. So either the front panel sensor or ETX sensor can turn the fan on. The only time the fan is off is when both sensors tell the fan it should be off.
 5. With the hardware change applied AND the EEPROM updated, software (as configured in the browser) determines if fan should always remain or should instead be controlled by the ETX sensor.
 - 6.
- **Mantis 3153** (written while 5.3.0 is shipping)

Summary: Please add fan control to TSync driver

Description: I have added a register at 0x0D0 to a special build of the FPGA which can turn the fan on and off. Writing a 0x0001 to the register will turn the fan on. Writing a 0x0000 to the register will turn the fan off. Bit 0 is the only bit that is active.

This will enable a daemon on the NWP to monitor temperatures in the unit and turn the fan on and off based on whatever algorithm we choose. The Front Panel will have to be modified to enable this feature (resistor change).

I would like to have HW_GetFan and HW_SetFan commands added to the driver. These commands are Lafayette-only and eventually would have to be added to the Lafayette patch.

- **ECN3381** (completed 3 Feb, 2014): Changed fan operating temp from 40C to 50C, and fan hysteresis from 10C to 2C
- **ECO195** (completed 27 Oct 2014): Changed fan operating temp from 50C back to 40C
- **ECO495** (completed 1 July, 2015): Changed fan hysteresis from 2C back to original 10C

Approximate Serial Numbers of all SecureSyncs between dates of ECN3381 and ECO195 (fan operating temp at 50C instead of 40C): 05408 – 07679 (~1633 units)

Of these 1633 units, 550 have a Rubidium oscillator installed.

Automatic thermal shut-down/operating in an “overtemp” condition

Operating temperature spec change

Email from Tony Diflorio to Hughes network (1/13/12)

This temperature spec was first changed in August 2010 – see attached datasheet from Aug 17, 2010 (rev F). Which is well before HNS selected Spectracom for the Jupiter project. Also, our engineers have informed me that the unit will operate at +70C, however, due to UL certification requirements the metal surfaces in the unit are not allowed to get above +70C and thus the reason for the change.

Q. Also can you provide information about what can be expected if the units are run beyond these limits? We do not intend to run them outside the range but we need to know the impact to the performance if the units are run beyond the limits.

(Email from Dave Sohn) Initially as the unit is heated above the temperature specification, the oscillator driving the timing system will become unstable. This instability will affect our timing performance and all output performance. As the unit continues to be heated, the unit will become unstable and unresponsive. On the low end, the first failure will be the front panel display failing to operate, and then the remainder of the unit will become unstable and unresponsive.

Note (internal use only at this time) apparently, the ETX has an over-temp protection that kicks in at 100 Celsius that significantly throttles back its operation/shuts it down.

However, it does have a temperature-operated cooling fan which turns on and off the cooling fan, based on the internal temperature. The temperature data calculated by the internal temperature sensor is not available to be reported by the SecureSync, so the internal temperature cannot be obtained from the appliance. The sensor is just used to control the cooling fan.

Email from Dave Sohn 3/28/11

The unit will always feel warm after a period of operation.
The fan should come on when the sensor is at +40C and shut off when the sensor is at +30C.

Note (3 Feb 2014 KW) Per Mark McGregor - ECN 3381 is changing the temp for fan operation added changes to decrease fan switch temperature delta for on to off from **10C to 2C**. Also changed fan turn on temperature from 40C to 50C. This was to minimize the frequency shift of the oscillator getting pushed around when the fan cycles and drives the temperature inside the box from 45C to 35C faster than the control loop can follow.

Note: Clarification to the SecureSync manual- the fan may not energize at power-up, if the unit wasn't running for about an hour or so prior to power-cycle. If the unit is cold at power-up, the fan won't run at start-up. But if it's warm, it will. (The internal temperature needs to be elevated above 30 Deg C to have the fan come on at startup).

To test the cooling fan operation, follow this procedure:

- 1) Power up the unit and allow it to warm up for about 30 minutes. This will raise the internal temperature to the operating range of the fan.
- 2) Turn off the power for about 5 seconds
- 3) Turn on the power and listen for the fan to come on. It will turn off after a short period of time unless the internal temp is above the fan shutoff level.

Issue with SecureSync booting back up again at the same temperature it was while it was running (observed long before Sept 2015/version 5.3.0 update) erratic front panel display observed

- Occurs if the temperature is near 55°C when the SecureSync is rebooted.
- If the ETX module has a chance to first cool down a few degrees, it will boot-up normally

Email from Dave Sohn (21 Sept 2015) This appears to be an issue with the ETX modules where they can run at high temperatures, but there is something restricting them from starting up at the same temperature. After the processor cools down for some short period, the system will start up again. We started talking with the manufacturer, Advantech, but I don't believe we have gotten far with that yet. It may also be worsened by some of the changes with the front panel fan operation that were shipping for a few months. This caused the fan to run less often.

As far as fixes, we are looking at changing the heat dissipation technique for the ETX. Currently we have a heat sink applied directly to the processor chip on the ETX, but a heat spreader is also available from the manufacturer that will pull the heat from the chip and spread it over a larger area. Operating at my desk, the overall temperature of the processor and ETX were lower by more than 5 degrees with the heat spreader. Whether we would work with just the heat spreader, or in combination with a heat sink remains to be seen. Alternatively, we are also looking at a newer ETX module from the vendor as well.

Example log entries from a unit with a CPU temp of 100 deg

- Refer to salesforce case 24138

Email from Dave L to Engineering (12 Jan 17) Here is a report of a Securesync that was updated from v 5.1.4 to 5.5.1 that has a high CPU Temp of 100 Deg. Also the GNSS 0 Reference keeps switching between Green and Dark on the HOME page. It should be going Green / Red, I see some of these strange messages in the System.log:

```
Jan 12 17:22:56 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 17:23:23 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:24:35 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
```

Jan 12 17:28:30 DC-NTP1 last message repeated 2 times
Jan 12 17:30:25 DC-NTP1 last message repeated 2 times
Jan 12 17:31:02 DC-NTP1 DC-NTP1: [webui: SPEC_KTSAL_EN=true XO_GetPhaseErrorLim 0 (KTSAL)
Jan 12 17:32:42 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:33:54 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:35:18 DC-NTP1 last message repeated 2 times
Jan 12 17:37:01 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:38:25 DC-NTP1 last message repeated 2 times
Jan 12 17:40:09 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:41:34 DC-NTP1 last message repeated 2 times
Jan 12 17:44:19 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:45:31 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:47:13 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:47:43 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 17:59:42 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:06:43 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:16:44 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:18:47 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:51:43 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 19:03:32 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 19:05:55 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 19:05:56 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 19:11:00 DC-NTP1 DC-NTP1: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetMode 0 (KTSAL)
Jan 12 19:13:44 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed: log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 19:15:33 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)

Reading/obtaining/storing internal temperatures

Regarding the front panel cooling fan

The Temperature reading for the cooling fan's operation is based on a temperature sensor located on the front panel assembly of all units. As of at least Oct 2015, this sensor's temperature reading for the fan operation is NOT reported anywhere (it's not one of the three temperatures reported in the browser with later software versions, for example). It just turns the fan on and off.

In summary: The temp sensors/read-outs discussed below are not associated with the cooling fan operation.

Storage of and obtaining reported/displayed temperatures

Storage of the temperature data

Length of time Temperature data is stored for:

- Refer to (in the SecureSync online user guide, then scroll down to "**Deleting Temperature Data**") http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

Email from Ron D (28 Mar 18) The temperature monitor graph page in the online manual states it. It should probably be added to all of the graph sections that it applies to.

Note- not edited to be directly sent to a customer- except

"Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten."

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

A) Via the CLI interface:

****Obtain Oscillator, board and CPU temperature readings via CLI (applicable to versions 5.4.5 and above only)**

- Version 5.4.5 added the **gettemp** command to allow reading of temperatures.

```
spadmin@Spectracom ~ $ gettemp

Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ gettemp
Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $ gettemp osc
N/A
spadmin@Spectracom ~ $ gettemp board
74.00 degrees C
spadmin@Spectracom ~ $ gettemp cpu
92.00 degrees C
spadmin@Spectracom ~ $
```

Q We would like a system status command via the CLI which gives up the temperature (“sensors” command on a Linux box)

A Email from Dave Sohn to Matt Loomis (8 Mar 16) “cat /sys/class/hwmon/hwmon0/temp*_input” run from the command line will provide the raw temperature monitor information from the processor board and CPU in that order. Divide by 1000 for degrees Celsius.

B) Via the web browser

Software version 5.3.1 and above (added System Monitor page)

- Version 5.3.1 moved the temperature graphs to the Tools -> System Monitor page of the browser



NOTE: from talking with Dave Sohn (22 oct 15 KW). These reported temperatures (in Celsius) may initially appear to be very hot to some customers. They need to understand that these are not ambient temperatures inside the chassis. They are the actual die temperature for the processor (Processor temp and CPU temp) or very close to the ovenized oscillator (Oscillator temp). These higher temps are expected for the specific components they are monitoring.

Note: all temperatures are calculated and reported in **Celsius**

C) “Oscillator temperature” (sensor “U60” located on the PCB very near the oscillator- not inside the oscillator. This was the first available temp readout - starting in software version 5.1.7)

Notes:

- The oscillator temp is not located inside any of the Wentzel oscillators, or any of our oscillators. It’s an ambient sensor located on the main board NEAR the oscillator. Ambient temp changes will inherently affect this temperature reading.
- Requires a hardware thermostat that started being installed on Rev B main boards back in 2012. Units purchased prior to Rev B (starting sometime in 2012) will not see these additions.
- This was the first temperature read-out available in the SecureSync.
- Per Paul Myers (in Mantis case) 9489s do not have the temperature sensor installed. Only SecureSyncs and 9483 purchased after sometime in 2012 have the sensor installed.
- Software version 5.1.7 and below don’t provide the means to report internal temperature (even if the sensor is installed)
- Software update version 5.2.0 added internal “temperature” readout (software support for an earlier hardware change of adding a thermostat that occurred sometime in 2012 with Rev B main boards)
- Typical temperature reading is around 50 degrees C.
- This temperature is measured near the oscillator, so its labeled changed from “*Temperature*” to “*Oscillator Temperature*” in later software versions.

Email Keith sent to a customer concerned about a .4 degree I spoke to one of engineers about what you are observing. He reminded me that it was important for you to understand that the reported Oscillator Temperatures are not obtained from a sensor within the oscillator itself. These readings are instead obtained from a sensor located on the main PCB board, near where the oscillator is located. So this sensor readings are affected by any ambient temperature changes to the internal air flow inside the unit. They are not a report of temperature fluctuations from within the oscillator itself (The oscillators used in the SecureSync do not report their internal temperatures. We just refer to this ambient air temperature reading as the “Oscillator temperature” because of where this sensor is located within the SecureSync).

The Wetzel oscillator in the Hughes SecureSync (and also the standard OCXO and Rubidium oscillators which can also be installed in SecureSyncs), is an ovenized oscillator, which helps it compensate for ambient air temperature changes. Changes in the oscillator’s DAC values are completely expected as its internal oven operates to keep the temperatures within the oscillator as stable as possible. The DAC changes are needed to steer the oscillator to 10 MHz as the internal temperatures waiver.

In summary, the “oscillator temp” is an ambient temperature reading taken near the oscillator. Changes of a few tenths of a degree in the ambient temperature are not at all unexpected and the oscillator’s internal over works to help dampen out the temperature changes inside the oscillator.

Storage/output of the three temperatures (and oscillator data) (via either a “.csv” or “.json” file)

All three available temperatures are stored in the SQLite database and can be downloaded as either a “.csv” file (for raw data that can be opened in excel) or a “.json” file (for raw graphing).

Download of raw temperate data as a “.csv” file (can be opened in excel)

- A “.csv” file with the three available temperatures can be downloaded in one of either two different methods

1. Download button available in the Management -> Disciplining page of the browser

From the **Management** -> **Disciplining** page of the browser (click on the “down arrow” icon on the right side of the page to download the .csv file. Press the garbage can icon to delete all of the oscillator and temperature data used to display the graphs)

2. Manually enter the link to the OscillatorStatusLog

If you manually enter **/logs/OscillatorStatusLog.csv** after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: <http://10.10.128.1/logs/OscillatorStatusLog.csv> (change address as applicable)

Example output below (“Sys temp” and “CPU temp” fields were added in software version 5.3.0)

id	sys timestamp	sync	holdover	time ref	pps ref	dac	phase error	freq error	sys temp	cpu temp	disc temp
63102	11/18/2015 15:45	0	0	gps0	gps0	32768	-15	0	81	100	0
63101	11/18/2015 15:43	0	0	gps0	gps0	32768	-15	0	81	100	0
63100	11/18/2015 15:42	0	0	gps0	gps0	32768	-15	0	81	100	0
63099	11/18/2015 15:41	0	0	gps0	gps0	32768	-15	0	81	100	0
63098	11/18/2015 15:40	0	0	gps0	gps0	32768	-15	0	81	100	0
63097	11/18/2015 15:39	0	0	gps0	gps0	32768	-15	0	81	99	0
63096	11/18/2015 15:38	0	0	gps0	gps0	32768	-15	0	81	100	0
63095	11/18/2015 15:36	0	0	gps0	gps0	32768	-15	0	81	100	0
63094	11/18/2015 15:34	0	0	gps0	gps0	32768	-15	0	81	100	0
63093	11/18/2015 15:33	0	0	gps0	gps0	32768	-15	0	81	100	0
63092	11/18/2015 15:32	0	0	gps0	gps0	32768	-15	0	81	99	0
63091	11/18/2015 15:31	0	0	gps0	gps0	32768	-15	0	80	100	0
63090	11/18/2015 15:30	0	0	gps0	gps0	32768	-15	0	81	100	0
63089	11/18/2015 15:29	0	0	gps0	gps0	32768	-15	0	81	98	0

Definition of fields

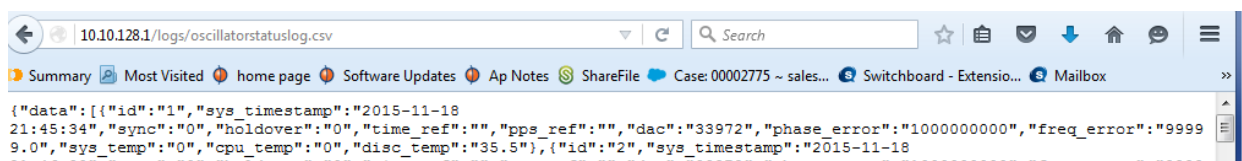
- **Sync** and **Holdover**: 1 is true, 0 is false
- **Time ref** and **PPS ref**: Selected input reference at that time
- **DAC**: Oscillator’s DAC value
- **Phase Error**: 1PPS Phase Error
- **Freq Error**: Oscillator’s Frequency Error
- **Temps**: Board, CPU and Oscillator
- **Notes**:
 1. **Oscillator** temp is only available if sensor is installed on the main PCB
 2. **Board** and **CPU** temps were added in software version 5.3.0

Output of graphable temperature and oscillator data (.json file)

- Same process as downloading.csv file, but replace “.csv” with “.json” instead.

If you manually enter **/logs/OscillatorStatusLog.json** after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

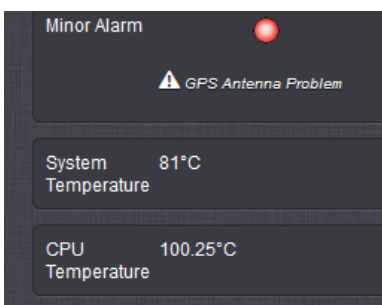
Example: <http://10.10.128.1/logs/OscillatorStatusLog.json> (change address as applicable)



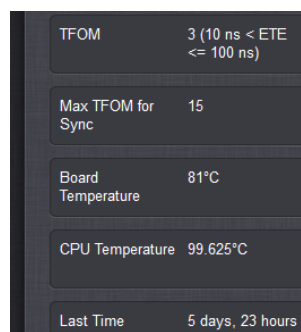
Processor board and CPU temperature graphs

Note about references to “temp sensor”: “Oscillator” temp is only available if the temperature sensor (U60) is installed on the main PCB (very close to the oscillator). Refer to ECN 2807 (5 Dec,2011)

- Software version 5.3.0 (Sept 2015) also added Board (System) Temperature and CPU temperature (three different temperatures are now available, for newer units that have the temp sensor installed)
- The CPU and board temperatures are not stored in discstats. All three temperatures are stored in MySQL database and can be downloaded as part of a csv or json file. See the information further above about how to export this raw data that is used for graphing.
- **CPU Temperature** and **Board Temperature** readouts added on the left side of the **Management -> Disciplining** page:
 - **System/Board Temperature** and **CPU temperature** readouts were added on the left side of the **Home** page, as well as the left side of the **Management -> Disciplining** page
 - **Home** page of browser



Management -> Disciplining page of browser



Summary of temperature readings/typical values (in blu)

- **With version 5.2.0, three different temperatures are now available, for newer units that have the temp sensor installed)**
 - **“Temperature” / “Oscillator Temperature”** = temperature sensor on PCB, near the oscillator (~ 50 deg c) (this was the first sensor reported - reported temperature was added in software versions 5.2.0/5.2.1, if the temp sensor is installed)
 - **“CPU Temperature”** = Processor temperature based on sensor near the KTS CPU processor (~100 deg C) (available in versions 5.3.0 and above)

Details of “CPU Temperature”

Partial email from Tim Hammer (24 Sept 2021) CPU Temperature is provided by a monitor built into the CPU chip. The CPU temperature will be similar to the Board temperature unless there is some CPU intensive activity occurring. During those times, CPU temperature will trend higher than the Board temperature.

- **“Board Temperature” / “System Temperature”** = **ETX module** temperature (~80 deg C) (available in versions 5.3.0 and above) via temp sensor within the ETX module (die temperature of the ETX module).

Details of “Board Temperature”

Partial email from Tim Hammer (24 Sept 2021) Board Temperature is provided by a monitor on the ETX (aka COM or SOM) board. This will be roughly the temperature inside the SS1200 enclosure.

Email from Dave L (17 Dec 2018) The CPU temperature can normally be 80 to 90 Deg C in units with older fan controls. This does not affect the CPU until it reaches temperatures **over 100 Deg C** where it will start throttling back to reduce power consumption and cool itself.

Rubidium oscillator equipped Securesync tend to run hotter. Your Securesyncs have the OCXO Oscillator option so they

characteristically have lower temperatures. The CPU Temperatures below 100 Deg would not be a major concern.

The cooling fan modification could be added but there is a cost and the units would need to be returned to Spectracom for the modification of approximately \$475 each. Since these are not over 100 Deg C there is no need to have the fan mod done in my opinion.

Temperature(s) displayed/reported/recorded:




- Only the temp sensor on the main board (if installed) is recorded in discstats (end of each entry)

16591,194,1,0,ird0,ird0,33384,15,8.94e-14,**59.597710**

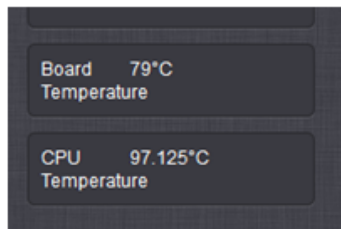
- The CPU and board temperatures are not stored in discstats. All three temperatures are stored in MySQL database and can be downloaded as part of a csv or json file. See the information further above about how to export this raw data that is used for graphing.

- **Report via SNMP:** As of at least v5.2.0, temperature doesn't appear to be available via SNMP.
- **Note:** Refer to Mantis case 1857.
- Displayed on the **Home** page of the newer browser (under "System Status" in the upper left corner)

Note: Temperature reports are not available in the classic interface browser

Versions 5.2.0 and 5.2.1 (if the temp sensor is installed)	Versions 5.3.0 and above (if the temp sensor is installed)	Software was updated to versions 5.3.0 and above (temp sensor was not installed)
		
<p>"Temperature" = temperature near the oscillator</p>	<p>"Temperature" = temperature near the oscillator</p> <p>"System Temperature" = ETX module temperature</p> <p>"CPU Temperature" = Processor temperature</p>	<p>Temperature near the oscillator not available without sensor installed</p> <p>"System temperature" = ETX module temperature</p> <p>"CPU Temperature" = Processor temperature</p>

Version 5.3.1 (if the temp sensor isn't installed)



"Board Temperature"= ETX Module Temperature

"CPU Temperature" = Processor Temperature

Note: **"Oscillator Temperature"** not available without sensor installed

Version 5.3.1 (if the temp sensor is installed)



"Oscillator Temperature" = Temperature near the oscillator

"Board Temperature"= ETX Module Temperature

"CPU Temperature" = Processor Temperature

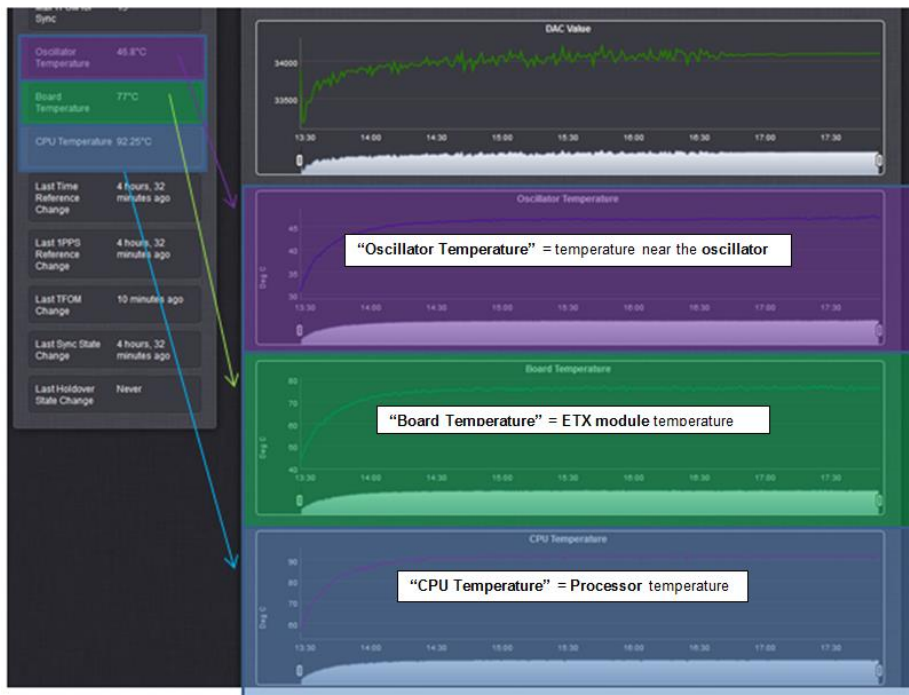
Issue: Reports/observations in our Engineering lab of CPU and other temperature graphs remaining exactly the same (~ March, 2017) after about four weeks of normal operation

- Reported/observed here ~Feb/Mar/Apr 2017 time-frame
- Refer to Salesforce case 23986 (for AOL)/ JIRA ticket SSS-253
- Temperatures vary/update for a few weeks after power-up, but then start remaining the exact same value (such as 23.725 degrees, for instance). Not the same on all units, but stops changing in each individual unit.
- Our Engineers found a unit here that is exhibiting this condition (end of Mar/first of Apr 2017).
- Fixed in update 5.7.0.

Fix: This issue was **fixed in the version 5.7.0** software update (we needed to change the speed of an ETX Monitoring bus to fix it).

Temperature-over-time graph (Management -> Disciplining page)

- Versions 5.3.0 and above (temp sensor installed)
- Reports Oscillator, board (ETX Module) and CPU (Processor) temperatures



Length of time the temperature data is stored for:

- refer to (in the SecureSync online user guide, then scroll down to "Deleting Temperature Data")
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

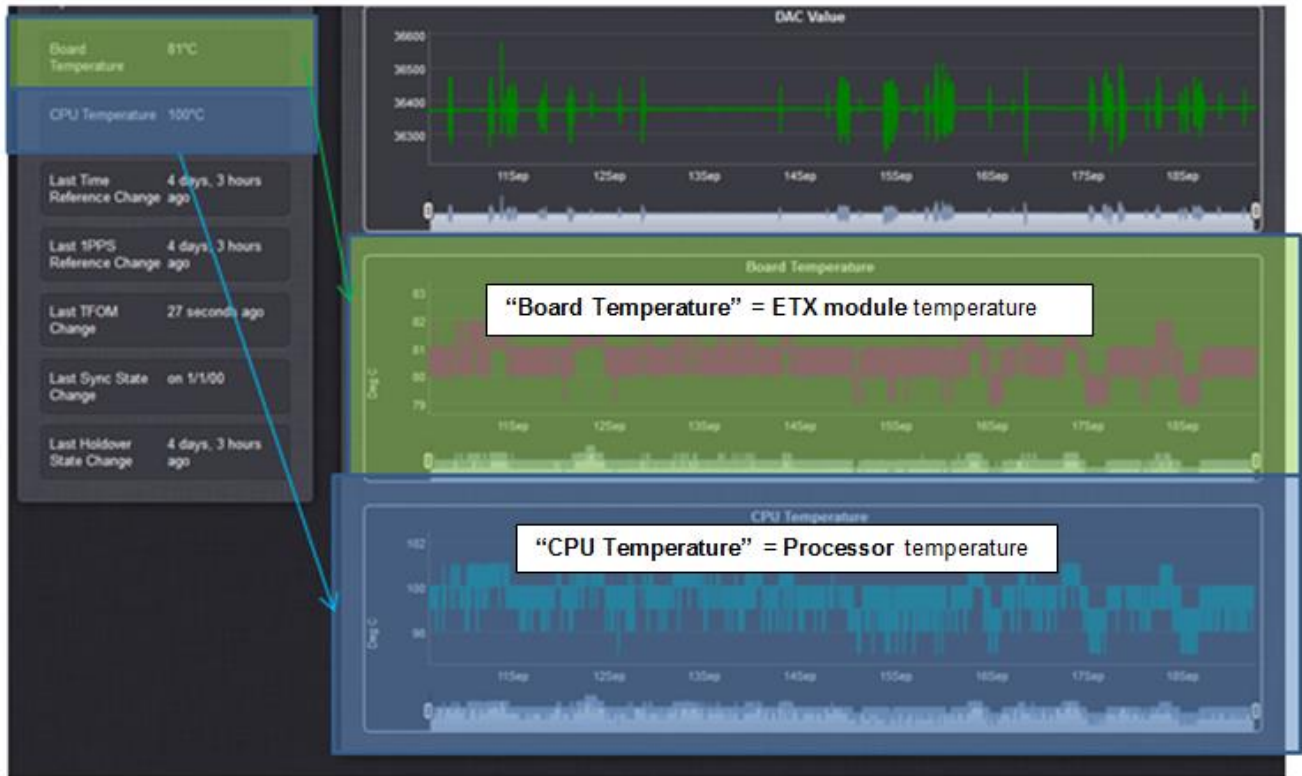
Email from Ron D (28 Mar 18) The temperature monitor graph page in the online manual states it. It should probably be added to all of the graph sections that it applies to.

"Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten."

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

Software was updated to versions 5.3.0 and above (and temp sensor was not installed)

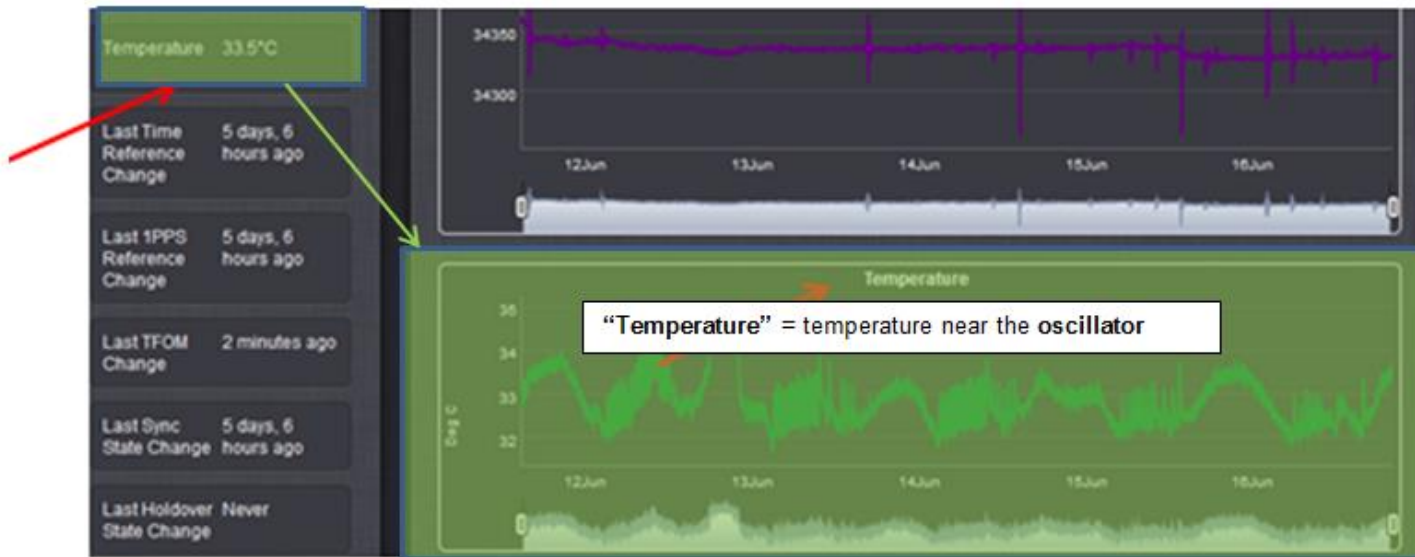
- Reports PCB and CPU temperatures (oscillator temp is not available without the sensor being installed and software versions prior to 5.1.7)



Temperature near oscillator not available without sensor installed

Versions 5.2.0 and 5.2.1 (if temp sensor is installed on the main board)

- Reports just oscillator temperature



Q. I'm trying to find out if SecureSync has a SNMP MIB variable to provide temperature? I have searched our SecureSync and Spectracom MIBs without finding anything so to be sure, I am asking

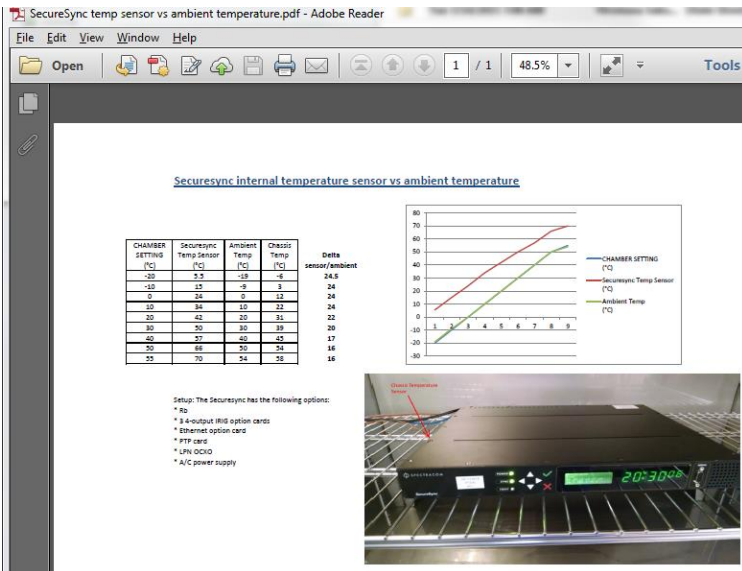
Update to the answer below (9 Dec 2015 KW). Software update v5.3.1 added objects for providing temperatures of the Oscillator, CPU and board (temp sensor on the front panel for the cooling fan isn't available via SNMP).

A (KW 11/8/12) with at least Archive versions 4.8.7 and prior, there is no way to read the internal temperature. Prior to Rev B of the main circuit board, there was no thermostat in the SecureSyncs. Rev B of the board adds a thermostat, but the software is not currently inter-operating with this component. Someday, we may integrate it into software. If we do, customers that apply the software update will have this capability available, if they have a rev B (or higher) circuit board installed.

Test data on the internal temperature sensor of the SecureSync vs ambient temperature

Q (from Raytheon) "for the temperature, I noticed that the probe is for internal to the system. At what reading would the temperature be considered critical? How does the operating temperature range in the spec correlate to the temp reading on the system?"

A Reply from Tim Tetreault (13 Jul 2015) Here is the test data on the internal temperature sensor of the SecureSync vs ambient temperature. The testing was done with a SecureSync that had the same configuration as the SecureSync's in the AMDR units.



Lithium coin cell Battery (or batteries) that may be installed / battery change intervals/ Shelf life

1. There is one Lithium battery in all SecureSyncs for the RTC (Real Time Clock) to keep it incrementing each second when the unit's primary power is lost.
 - Refer to the ETX battery section further below for details on this battery: [ETX module/ BIOS/ CF Card RTC \(Real Time Clock\) / kernel time at boot-up/ coin cell battery / Shelf Life](#)
2. If a GB-GRAM Receiver (Model 1204-1A Option Card) is installed, it also has one lithium battery installed
 - Refer to the separate "Model 1204-1A GB-Gram Option card 12" document for details on this battery: [U:\Engineering\SAASM-FOUO\CustomerService\SecureSync](#)

In summary of the info above:

Either one or two batteries are installed in SecureSync:

- There is just one lithium battery is installed if GB-Gram SAASM receiver is not installed (the lithium battery for the RTC)
- Two batteries are installed if GB-GRAM SAASM receiver is installed (one lithium battery for the RTC and the other lithium battery is for the receiver)

Main PCB Board/Flash memory

Flash memory

A) ECO-001556 (SecureSync main board update to new Flash)

- Refer to (in Arena): https://app.bom.com/changes/detail-summary?change_id=2392738945&

Description

New KTS software will be required to work with the new Flash. Software has already been tested and verified in the TSync-PCI update so this should be very low risk.

U5 from U060R-F640-000P to U060R-F128-000P addressing ECR-000236.

C101R-0102-YK0B, C409 added DNP, R328 added R116R-0000-YJ0B, R329, R330, R331, R332 added.

Updated Assembly Drawing and Drill drawing notes to latest spec's.

Addressed ECR-000034.

There should be no changes required to the PD's or TP's.

ETX module/ BIOS/ CF Card/ RTC (Real Time Clock) / kernel time at boot-up/ RTC coin cell battery / Shelf Life

ETX module (SBC- Single Board Computer)

- ETX module is used with SNMP, NTP (one of the higher priorities in the system), Apache web browser, oscillator disciplining, alarm monitoring and notifications, front panel, GPS monitor, etc (items that are displayed in the “top” and “rc-status” cli commands

Location of / reseating of ETX module

- If eth0 not working for instance, ETX should be reseated

Email from Jodi to customer (28 Sept 17) There is a possibility that the problem could be that that ETX module is not fully seated within the SecureSync. Are you able to—do you have permissions to—remove the cover and press down on the center of the ETX module to make sure it's fully seated? If so, I can send more information on that.

Email from Jodi to customer (28 Sept 17) The ETX module is located near the CF card. It has 4 screws and a black heat sink. Remove power from the Secure Sync first, of course. Once you remove the cover of this SecureSync, we recommend following best practice for ESD environments. Remove the screws from the ETX module, take the module out, then re-seat it and replace the screws. Once you've ensured that it's fully seated, you can then put the cover back on and start the device up again.

A) **SOM-4466TZ2-T01A1E** (2nd generation ETX for SecureSyncs and 9400s)



Associated ECOs for the upgrades:

- ECO 1330 (Aug 2017) is to incorporate the 2nd gen ETX in SecureSyncs): in Arena https://app.bom.com/changes/detail-summary?change_id=2389332675&
- ECO 1294 (Aug 2017) is to incorporate the 2nd gen ETX in 9400 series NetClocks): in Arena: https://app.bom.com/changes/detail-summary?change_id=2388757395&orb_msg_single_search_p=1

Mfg: Advantech

MFG P/N SOM-4466TZ2-T01A1E

Mfg datasheet: http://www.advantech.com/products/1-2jkpap/som-4466/mod_543c267b-0357-47cc-a388-86c0383f1c9d

Our Part Numbers

1. For SecureSyncs: MP20R-0003-0010

2. NetClock Models 9483 and 9489

- Implementation of new ETX into NetClocks is later than with SecureSyncs
- **Cut-in S/N for 9400s (ECO 1294)** is: ?? (sometime after 23 Aug 17- the date this ECO was “completed”)

How to tell if a 2nd generation ETX is installed

1. Serial Number
2. Date of shipment is an approximate way to tell
3. The manifest.log (applicable only to v5.7.1 and above only)

Specs for the 2nd gen Advantech ETX modules

- Refer to sites such as: http://www.advantech.com/products/1-2jkpap/som-4466/mod_543c267b-0357-47cc-a388-86c0383f1c9d
- link to Datasheet” [https://advdownload.blob.core.windows.net/productfile/PIS/SOM-4466/Product%20-%20Datasheet/SOM-4466_DS\(01.14.16\)20160114103018.pdf](https://advdownload.blob.core.windows.net/productfile/PIS/SOM-4466/Product%20-%20Datasheet/SOM-4466_DS(01.14.16)20160114103018.pdf)

Common specs for the ETX used in SecureSyncs and ETX used in NetClock 9400a

- Frequency/RAM: AMD T16R **615** MHz/Single Core/512 K

Differences between the ETX module for SecureSync and one for NetClocks (temperature rating is only difference):

1. **MP20R-0003-0010 (for SecureSyncs)**
 - Module, CPU, ETX, AMD G-Series, **-40 to +85C** with 2G memory
2. **MP20R-0003-0011 (for NetClock 9400 series)**
 - Module, CPU, ETX, AMD G-Series, **0 to 60C** with 2GB memory

Software version requirements for the 2nd gen ETX module

- Cannot downgrade to a version prior to version 5.7.0 (5.7.0 and above support the newer ETX).

Note: Timekeeper option is not compatible with the newer generation ETX (units with this option enabled must remain with the first generation ETX module installed)

B) **SOM-4455Z-T01A2E** First generation (1st gen) ETX modules (SecureSyncs, 9400s and 9383/9389)

- **Mfg:** Advantech
- **Mfg P/N:**
 - **SOM-4455Z-T01A2E** (extended temp)
 - **SOM-4455R-T01A2E** (standard temp)

Our P/Ns:

1. **MP20R-0003-0008: MODULE,SBC,ETX,512MB RAM, -20C to 80C (extended temp for SecureSyncs)**
 - **In Arena at:** https://app.bom.com/items/detail-spec?item_id=1202844918&version_id=10299163988&orb_msg_single_search_p=1
2. **MP20R-0003-0006: MODULE,SBC,ETX,512MB RAM, (Standard temp for 9483/9489)**
3. **MP20R-0003-0009 MODULE,SBC,ETX,512MB RAM, Long Conn (standard temp for 9383/9389)**

Q. What is the PROCESSOR(cpu) and Clock rate of SecureSync? (Ex.: Geode LX800 with 500MHz)

A. Reference: http://www.advantech.com/products/SOM-4455/mod_37BFA971-A650-4458-9588-F569B005CF78.aspx.

CPU: Embedded AMD Geode™ LX800 CPU+ AMD CS5536 Chipset

Q. Question from Dick Fox (1/5/12) Do we have a spec on the CPU speed and memory that we can share?

A. Email reply from Dave Sohn The SecureSync CPU runs at 500MHz an APO calls d has 512MB RAM.

ETX general info

- **Manufacturer:** Advantech

Second generation ETX module (4466) MP20R-0003-0011

P/N: MP20R-0003-0011 (in Arena) https://app.bom.com/items/detail-spec-redline?item_id=1229598775&version_id=10679427568&&redirect_seqno=10289971298

Description: Module, CPU, ETX, AMD G-Series, 0 to 60C w 2GB memory

C) ECO-1294 (Aug 2017) update ETX module in Netclock to 4466 (2ND GEN ETX)

https://app.bom.com/changes/detail-approvals?change_id=2388757395

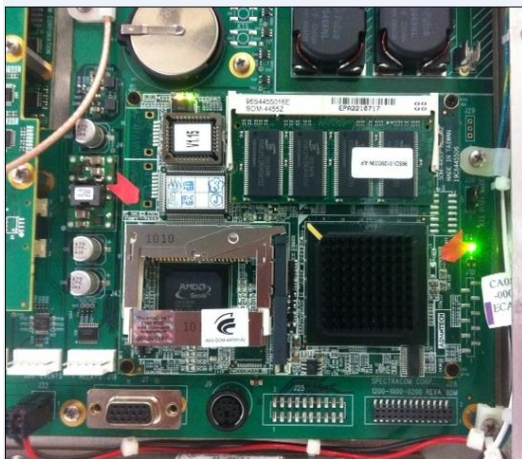
Change ETX from MP20-0003-0006 to MP20R-0003-0011

Change ETX from MP20-0003-0006 to MP20R-0003-0011

Change ETX mounting screws from HM11R-25R4-0005 to HM11R-25R4-0012

remove heat sink MP12R-0004-0002

First generation ETX module



(Advantech P/N SOM-4455ZR-T01A2E)

Our P/N: MP20R-0003-0008

- **Main link for data sheets manuals, etc :** www.advantech.com/products/1-2JKPAP/SOM-4455/mod_37BFA971-A650-4458-9588-F569B005CF78.aspx
- **Data Sheet:** http://downloadt.advantech.com/ProductFile/PIS/SOM-4455/Product%20-%20Datasheet/SOM-4455_DS%2801.15.14%2920140205153221.pdf

MAC address

- Originally, MAC address was always "00:d0"

- Change to “74:fe” was APPROXIMATELY in Aug, 2015

Partial email from Open Access/ASX (Aug, 2015) (At that time, Manufacturing had some units with each MAC Address formatting)

Old securesync: 00:d0:c9:d9:e8:74
Another old one: 00:d0:c9:c9:58:2b
New securesync: 74:fe:48:07:77:37

ETX seating

- Symptoms of ETX module may not be fully seated
- Eth0 IP address 0.0.0.0
- Eth0's Static IP address not being retained.
- Boot-up issues.

Email from Dave Lorah (18 Nov 2013) There is a chance the computer module has a poor connection to the motherboard. Maybe pressing on the connectors to reseat them would fix the problem. This would require you remove the top cover and press down firmly on the edges of the computer module to make sure they are all seated fully. If the SecureSync suffered a lot of vibration or a large physical shock during shipping it might have loosened this connection.

To remove the top cover, remove the 20 screws around the edge and lift the cover. Then firmly (but not too hard) press on the edges of the computer module to make sure the connector is seated. Attached is a photo of the computer module. Press along the edges indicated by the red arrows in the photo.

Location of and reseating of ETX module

- If eth0 not working for instance, ETX should be reseated

Email from Jodi to customer (28 Sept 17) There is a possibility that the problem could be that that ETX module is not fully seated within the SecureSync. Are you able to—do you have permissions to—remove the cover and press down on the center of the ETX module to make sure it's fully seated? If so, I can send more information on that.

Email from Jodi to customer (28 Sept 17) The ETX module is located near the CF card. It has 4 screws and a black heat sink. Remove power from the Secure Sync first, of course. Once you remove the cover of this SecureSync, we recommend following best practice for ESD environments. Remove the screws from the ETX module, take the module out, then re-seat it and replace the screws. Once you've ensured that it's fully seated, you can then put the cover back on and start the device up again.

ETX BIOS

- For info on replacing the BIOS battery, refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement](#)

Software update version changes associated with BIOS

- **Version 5.6.0** (Apr 2017) added ability for the software update process to be able to program BIOS changes.

BIOS changes

A) BIOS change for Harris update version 5.8G (5.8.G) (and now, as well as versions 5.8.9 and above)

- **JIRA SSS-832:** "Set Securesync 1200 BIOS CPU / RAM speed from auto to 500 MHz"

B) ETX BIOS change for 2nd generation ETX (Advantech SOM-4466)

1. BIOS revision is I1.12 (June 2019)

- Refer to ECO-FAI-001968 (in Arena): https://app.bom.com/changes/detail-summary?change_id=2395946350&

- Excerpt below:

Update BIOS in Advantech 4466 ETX modules to stop the failure to boot if there is no backup battery or the battery is dead. The jumper on the module must also be moved from pins 1 and 2 to pins 2 and 3 on the ETX modules.

New BIOS revision is I1.12

*Part Number: 1420046144

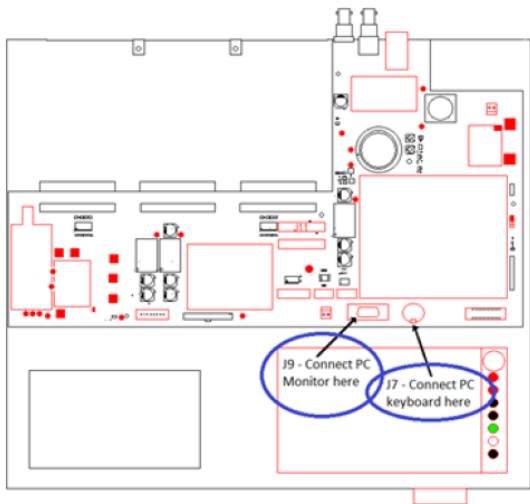
*Description: BIOS SOM-4466 I1.12 CS: C9F2 MX25L3206EM2I-12G

- ECO completed/effective date: 28 May 2019
- BIOS update files/procedure (in Arena): https://app.bom.com/changes/detail-attach?change_id=2395946350

ETX Bios memory: 512 kB (4 Mbit) Flash BIOS

Desire to view the BIOS

Email from /Dave Lorah- These items are you standard VGA cable and Keyboard cable, I have attached the jpegs for your review



BIOS protection against viruses

Q. Do we protect BIOS from potential viruses and possible corruption?

A Reply from Mark Goodlein (3/21/12) Our system is running Linux and the permissions have been locked down for security to protect it from viruses. In order for a virus to attack the BIOS, it would require superuser access, which has been locked down.

Q. Do you support a Secure BIOS Ecosystem?

- Digital signature that ensures Firmware/BIOS/Image authenticity.
- Root of trust for updates. contains signature verification algorithm and a key store that includes a public key to verify the signature or include a hash of the public key if a copy of the public key is provided with the BIOS update image
- Authentication BIOS mechanism.
- Do you have a protection mechanism?

Local Updates

- Ensures authenticity and integrity of the update image by requiring physical presence
- Supply chain ensures a secure, trusted or attested to BIOS
- The supply chain and custody process is documented
- Restriction of remote upgrades via a network

A Reply from Mark Goodlein (3/21/12)

Our BIOS is flashed by the vendor then configured here in manufacturing. We do not currently support updates to the BIOS nor have we ever needed to. I do not believe we have a "Secure BIOS Ecosystem" or any specific protection mechanisms in place.

For ETX BIOS configuration, refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\ETX BIOS settings](#)

NOTE: SecureSync boots-up using the ETX BIOS settings for its starting Time/Date values (BIOS time is "loosely" maintained by the RTC in the ETX module, as described further below).

Default BIOS settings: 2003/1/1 00:00. (year 2003)

Note: If the default BIOS date/time are displayed after each power-up:

- BIOS (lithium coin cell) battery may be bad. TP69 should be around 3 vdc with a good battery installed. Refer to: Shelf Life/Internal coin cell battery further down in this document.
- ETX module was removed/reinstalled without the BIOS being correctly configured.
- The BIOS was not set correctly at the factory prior to shipment.

Q. If the power is turned OFF and ON, the date and time of SecureSync are reset. Is it possible to make a setting so that SecureSync recovers with the date and time close to the time when the power was turned OFF?

A. SecureSync will load the system time from a battery backed clock each time it powers up. The unit will still not be in sync until a valid reference is applied, however. We are going to be adding a feature that will allow a user to select a mode where that battery backed time write also synchronizes the unit.
(update 10/28/12-Battery Backed time was added in V4.8.0).

ETX Ethernet drivers for Eth0 (E100 and 8139too)

- Two Ethernet drivers are loaded for the ETX module/Eth0.
- They are the E100 and 8139too Ethernet drivers

As shown with **cat proc** command, two Ethernet drivers are loaded for Eth0. They are E100 and a Realtek 8139TOO (or 8139T00). They are both installed because one is for one type of ETX and the other is for a different type of ETX module.

Ethernet driver updates for eth0 incorporated

- Update version 5.3.0 updated the Ethernet “8139too” driver to version 0.9.88 to improve operation of eth0
 - This was to fix the issues with eth0 potentially hanging/locking up if the port is set to 10/half (for example, it couldn’t negotiate with its switch).
 - **From the Release Notes:** “Updated to 0.9.88 version of 8139too Ethernet Eth0 10/100 driver”
- Update version 5.3.0 updated the Ethernet driver to improve performance of Eth0.
 - **From the Release Notes:** “Gigabit Ethernet Option Card: Updated Gigabit Ethernet driver to version 3.1.0.2”

8139too.ko (in kernel log)

- Per Ron, Not an issue if a 2nd generation ETX module is installed

```
spadmin@4 /lib/modules/4.14.34-gentoo-x64 $ find /lib/modules/ -name 8139too.ko  
/lib/modules/4.14.34-gentoo/kernel/drivers/net/ethernet/realtek/8139too.ko
```

```
spadmin@4 /lib/modules/4.14.34-gentoo-x64 $ find /lib/modules/ -name e100.ko  
/lib/modules/4.14.34-gentoo-x64/kernel/drivers/net/ethernet/intel/e100.ko  
/lib/modules/4.14.34-gentoo/kernel/drivers/net/ethernet/intel/e100.ko
```

Email from Ron Dries (3 Dec 2018) The 8139too error is not an issue. The newer (64 bit, instead of 32 bit) ETX module does not use it and it appears he has the newer ETX module.

**Indications of a potential ETX module failing or issue with the CF card:

- 1) Stalls during boot-up
- 2) Keypad not responding
- 3) Random unexpected rebooting

- 4) * LCD blank but LED clock counting up.
- 5) Sync / Fault LEDS not working
- 6) Can't login to browser or CLI
- 7) * Issues with Eth 0 intermittent/not working (eth1, eth2 and eth3 if installed, operating just fine)
- 8) Front panel Serial "**Console**" port is not responding.
- 9) "When the system try to boot up it look for the file "/dev/tsyncpci" file but failed and keep looping for that file."
- 10) Review the kernel log (**kern.log**) in the log bundle for the following type entries (especially "**segfault**" "**call trace**" "**BUG**" "**inode**", "**tainted:**" "**oops**" entries).

```

Sep 9 10:17:12 RC-GPSNTP01 kernel: BUG: unable to handle kernel NULL pointer dereference at 00000028
Sep 9 10:17:12 RC-GPSNTP01 kernel: IP: [<00000028>] 0x27
Sep 9 10:17:12 RC-GPSNTP01 kernel: *pde = 00000000
Sep 9 10:17:12 RC-GPSNTP01 kernel: Oops: 0000 [#1] PREEMPT
Sep 9 10:17:12 RC-GPSNTP01 kernel: Modules linked in: e1000e(O) 8139too e100 tsyncpci(O) pps_core
Sep 9 10:17:12 RC-GPSNTP01 kernel: Pid: 8535, comm: sh Tainted: G      O 3.8.13-gentoo #1 /AMD-GX3
Sep 9 10:17:12 RC-GPSNTP01 kernel: EIP: 0060:[<00000028>] EFLAGS: 00010202 CPU: 0
Sep 9 10:17:12 RC-GPSNTP01 kernel: EIP is at 0x28
Sep 9 10:17:12 RC-GPSNTP01 kernel: EAX: d4d684d0 EBX: dbfaffb4 ECX: ded98820 EDX: 58deea96
Sep 9 10:17:12 RC-GPSNTP01 kernel: ESI: b752f9e0 EDI: c1021e50 EBP: dbfaffa4 ESP: dbfaff34
Sep 9 10:17:12 RC-GPSNTP01 kernel: DS: 007b ES: 007b FS: 0000 GS: 0033 SS: 0068
Sep 9 10:17:12 RC-GPSNTP01 kernel: CR0: 8005003b CR2: 00000028 CR3: 1be71000 CR4: 00000090
Sep 9 10:17:12 RC-GPSNTP01 kernel: DR0: 00000000 DR1: 00000000 DR2: 00000000 DR3: 00000000
Sep 9 10:17:12 RC-GPSNTP01 kernel: DR6: ffff0f0 DR7: 00000400
Sep 9 10:17:12 RC-GPSNTP01 kernel: Process sh (pid: 8535, ti=dbfae000 task=deea96c0 task.ti=dbfae000)
Sep 9 10:17:12 RC-GPSNTP01 kernel: Stack:
Sep 9 10:17:12 RC-GPSNTP01 kernel: 00000010 dbfaff48 deea96c0 ded98858 dbfaffb4 ded98820 00000028
00000004
Sep 9 10:17:12 RC-GPSNTP01 kernel: dbfaff80 c109f0b6 00000001 00000000 00000000 d4c3f908 dec0d8d0
de8e8800
Sep 9 10:17:12 RC-GPSNTP01 kernel: deea9960 deea96c0 00000000 dbfaff88 c109f228 dbfaff9c c10404a6
00000002
Sep 9 10:17:12 RC-GPSNTP01 kernel: Call Trace:
Sep 9 10:17:12 RC-GPSNTP01 kernel: [<c109f0b6>] ? __fput+0x126/0x1f0
Sep 9 10:17:12 RC-GPSNTP01 kernel: [<c109f228>] ? ____fput+0x8/0x10
Sep 9 10:17:12 RC-GPSNTP01 kernel: [<c10404a6>] ? task_work_run+0x66/0xa0
Sep 9 10:17:12 RC-GPSNTP01 kernel: [<c1021e50>] ? vmalloc_sync_all+0x150/0x150
Sep 9 10:17:12 RC-GPSNTP01 kernel: [<c1021e58>] do_page_fault+0x8/0x10
Sep 9 10:17:12 RC-GPSNTP01 kernel: [<c1331cdc>] error_code+0x58/0x60
Sep 9 10:17:12 RC-GPSNTP01 kernel: [<c1021e50>] ? vmalloc_sync_all+0x150/0x150
Sep 9 10:17:12 RC-GPSNTP01 kernel: Code: Bad EIP value.
Sep 9 10:17:12 RC-GPSNTP01 kernel: EIP: [<00000028>] 0x28 SS:ESP 0068:dbfaff34
Sep 9 10:17:12 RC-GPSNTP01 kernel: CR2: 0000000000000028
Sep 9 10:17:12 RC-GPSNTP01 kernel: ---[ end trace 36560a0db060e9c7 ]---

```

inode entries "RC-GPSNTP01 kernel: ext3_orphan_cleanup: deleting unreferenced inode 9967"

Example from a unit that may have a bad ETX:

```

Oct 21 21:12:32 RC-GPSNTP01 kernel: ext3_orphan_cleanup: deleting unreferenced inode 99679
Oct 21 21:12:32 RC-GPSNTP01 kernel: ext3_orphan_cleanup: deleting unreferenced inode 99678
Oct 21 21:12:32 RC-GPSNTP01 kernel: ext3_orphan_cleanup: deleting unreferenced inode 99677
Oct 21 21:12:32 RC-GPSNTP01 kernel: ext3_orphan_cleanup: deleting unreferenced inode 99676
Oct 21 21:12:32 RC-GPSNTP01 kernel: ext3_orphan_cleanup: deleting unreferenced inode 99675
Oct 21 21:12:32 RC-GPSNTP01 kernel: EXT3-fs (hda1): 5 orphan inodes deleted

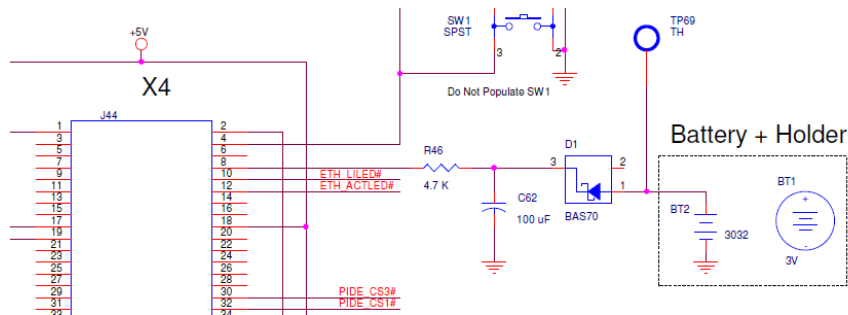
```

RTC coin cell lithium battery (BR3032)

- Info/Document for replacing the RTC battery in SecureSync (P/N 1200-5000-0055)
 - Refer to manuals in Released drive: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement](#)



- There is one lithium battery installed on the main PCB in all SecureSyncs. This is for the BIOS/RTC clock (A 3vdc - 500mAh, Lithium coin cell battery)
- The battery just allows the RTC clock to keep incrementing the time while input power is not available. It isn't used to store the time at all.
- The battery only discharges when input power is removed.
- If the battery is removed or its voltage drops too low, the worst thing that happens is the RTC doesn't increment while power is removed. So it will power-up with whatever the time/date was when it was last set. The amount of initial error is about the amount of elapsed time it was powered-down. If it was powered-down for 10 minutes, the time would be about 10 minutes or so off at power-up. It doesn't prevent the time from being changed from the incrementing 0's at start-up.
- Except for the time/date (which defaults to the year 2003 if the battery is removed), the BIOS settings now only need to be reset if the ETX module is removed. All other BIOS settings persist in Flash memory.



BR3032 Battery manufacturer: Panasonic

- **MSDS and other info:** <https://industrial.panasonic.com/ww/products/batteries/primary-batteries/lithium-batteries/coin-type-lithium-batteries-br-series/BR3032>

Email from Dave L (12 Feb 18) Here is the web page for the batteries. You can get the product safety data sheet from the bottom of this webpage:

<https://industrial.panasonic.com/ww/products/batteries/primary-batteries/lithium-batteries/coin-type-lithium-batteries-br-series/BR3032>

Manufacturing test of the battery (TP69)

Q What test point is the voltage of the coin battery in the attached test report?

A Test point 69 is used to test the voltage of the battery during production.

The coin cell battery voltage is checked during production functional testing. Mainboards with batteries containing a voltage less than or equal to 3.0VDC are removed for disposition according to Orolia's MRB process.

Recommended RTC battery voltage range (minimum voltage)

Per Tom Richardson (Oct 2014)

I found it in one of the design guides.

BATT Input=

3V backup cell input from carrier to SOM-ETX module for RTC operation and storage register non-volatility in the absence of system power. (BATT=2.4V-3.3V)

So it looks like 2.4 is the minimum.

Methods to tell if the RTC battery needs to be replaced

Q. how does the operator/maintainer know the battery needs to be replaced? Is there a way to use the software to check the battery levels?

A. reply from Keith (Oct 2014) To answer your question, there are really only two ways to tell if the Lithium coin cell RTC battery needs to be replaced. The first is the System Time will be incorrect at each power-up, with the amount of error being about the length of time it was powered-down for, until an external reference corrects the time and the SecureSync goes into Sync. The second way is to measure the voltage on the battery with the cover removed (there is also a test point on the main board for this voltage, TP69).

The battery has an expected life of about 5 years of cumulative unit power-down time (it only discharges when input power is removed from the SecureSync). As long as power is normally applied, I would recommend that the battery just be routinely replaced like every 5 years or so to prevent it from starting to become too low.

FYI- the coin cell BIOS battery is not considered critical to the SecureSync's operation. Its only function is to keep the Real Time clock incrementing when power is removed. The Real Time Clock is the start-up time reference for the system until an external time reference becomes present and valid to correct any time errors, before SecureSync goes into sync.

Note: With the exception of the ETX module and battery/socket, the rest of the components associated with the coin battery are attached to the bottom of the main SecureSync PCB. The stand-offs need to be removed to allow access to the bottom of the PCB board.

C62 is a Bypass Capacitor for Noise. It is also for charge storage to keep the battery voltage up while the batter is being changed if the battery is not dead.

The battery is present to keep the ETX single board computer internal clock/date in stored memory should SecureSync power cycle. After power has returned the SecureSync will display BIOS time. The unit will update (+/- adjusted seconds) the displayed time upon normal GPS reception. A battery circuit failure will not affect GPS and/or Oscillator and Sync functions.

Please inform the customer that the SecureSync is not broken if the battery fails. It will operate properly without the battery. The SecureSync is still functional even with the ETX backup battery failed. The battery is only used when power goes down and the SecureSync has no power applied. The only effect of the failed ETX backup battery will be that it will take longer to Sync after power is re-applied. It will also not remember the time and date, etc., but will get it from the GPS.

The battery being dead is not a critical failure as if the SecureSync won't operate because the backup battery is dead.

Does the customer connect the SecureSync power into an Uninterruptible power supply?

BR3032 battery reportedly discontinued

- Refer to Salesforce Case 291876 (Dec 2022)

From: <https://www.batteriesinflash.com/regular-rechargeable-batteries/coin-cell-battery-cr3032-3v-lithium-replaces-dl3032-br3032-kl3032>

Q What battery can replace BR3032?

A Coin Cell Battery CR3032 3V Lithium

Coin Cell Battery CR3032 3V Lithium, Replaces DL3032, **BR3032**, KL3032.

Effects on the system if RTC Lithium coin cell battery is removed or dead,

- Effects on system depend on which generation ETX module is installed:

A) 2nd Gen ETX module installed (blank LCD and blank LED. Need to power cycle twice)

- ETX modules from Advantech (with a revised BIOS and a jumper in a different location), the unit will initially “hang”, if the battery is dead or removed. But if its them powered-down and then quickly powered-back up right away again, it will be able to power up again.
- ~~We are supposed to at some time start receiving the ETX modules with a different BIOS/jumper setting which alleviates this conditon. This issue applies the first unit shipped with the 2nd gen ETX module, through the first unit shipped with the bios/jumper modified ETX (sometime post Jan 2019).~~—Status update to this potential change/fix, Per Ron Dries (18 Nov 2021) We tried to use a ETX that had been modified by Advantech, but it hjust caused more problems. So we reverted back.



Specific Reason for the need to power cycle twice

- Refer to Salesforce case 268696
- When the EX detects a bad or missing battery, the ETX halts its boot-up process (with a confirmation request to continue). The subsequent power cycle overrides the halt/confirmation and thus allows the ETX module to continue booting-up.
- To alleviate the requirement of the second/subsequent power cycle, change (or install) the coin cell battery.

Per discussion with Ron Dries (18 Nov 2021) when the ETX first powers-up and sees its battery is either dead or missing, it asks for a confirmation on whether or not to proceed with booting-up. If it doesn't receive the confirmation, it just sits there waiting for it. The second power cycle overrides the need to respond with the confirmation.

~~~~~  
**Report from Keith to Ron Dries (1 April 2020)** A quick, very preliminary report of something we've just started noticing. We've received a couple recent reports of SecureSync customers swapping out their CF card with ones we sent (should be 5.8.8) that aren't consistently booting-up, once new card is installed.

Below is an RMA I just issued for two units exhibiting this. And Denise just got off the phone with BAE with this report. Didn't boot the first time but booted ok the second.

If the lithium battery has failed, can it cause any intermittent issues with boot-up? Or just the first boot after its been replaced on 2<sup>nd</sup> gen ETX. We will get logs/configs to see what they show.

**Reply from Ron Dries (2 Apr 2020):** With the 2nd gen ETX if the lithium battery isn't present or needs to be replaced, the SecureSync power switch would need to be turned on, then off and back on again for the unit to boot.

#### Other associated messages

**Associated report from customer Jeff Edelson:** "We have two units to send in. Neither will boot consistently. One boots every third time you turn it on."

**Per Dave Sohn (24 May 2019)** "SecureSyncs with newer ETX board will not complete power-up with a dead or removed RTC battery."

**Per Ron Dries (1 Feb 2019):** if the ETX battery fails with a 2nd gen ETX module (at least until we start receiving 2nd gen ETX modules from Advantech with a revised BIOS and a jumper in a different location), the unit will initially "hang", but if its them powered-down and then quickly powered-back up right away, it will be able to power up again.

~~We are supposed to at some time start receiving the ETX modules with a different BIOS/jumper setting which alleviates this condition. This issue applies the first unit shipped with the 2nd gen ETX module, through the first unit shipped with the bios/jumper modified ETX (sometime post Jan 2019).~~

**Status update to this potential change/fix, Per Ron Dries (18 Nov 2021)** We tried to use an ETX that had been modified by Advantech, but it just caused more problems. So we reverted back.

---

## B) 1<sup>st</sup> Gen ETX module installed

- The only setting lost when the battery is removed is the RTC clock (date/time). All other BIOS Settings and System Settings (network, NTP, Reference Priority) are stored in Flash memory and are not lost when the battery is removed.

Q. If we remove and reseal "button battery" on the SecureSync and re-set clock by configuring the BIOS settings, will each setting(ex, IP address, NTP setting, reference setting etc,) be initialized?

A. **Reply from Keith (11 Nov 2014)** The very short answer to your question is "no". Each setting (ex, IP address, NTP setting, reference setting etc,) will not be initialized after removing/reinstalling this battery.

I confirmed with our Engineering team what the effects are of removing the ETX's Real Time Clock coin cell battery. The only setting lost when this battery is removed is the approximate date/time for the next time the unit is booted-up. The BIOS date/time can be reprogrammed after re-installing the battery if you wish. If this setting isn't reprogrammed with a keyboard and monitor attached to the main board, it will take a little longer for the SecureSync to power-up and sync just the next time its powered-up and synced to GPS. And it will power-up the first time with the incorrect date and time. However, within about 10 minutes or so of the SecureSync resyncing to GPS, NTP or other external time reference, the Real Time Clock for the ETX module will be automatically updated with the correct time/date (just as if the BIOS had been updated with a keyboard and monitor). All other settings for the unit besides the time/date at next power-up (such as the network and NTP settings, Reference Priority table, etc) are stored in a CF flash card that doesn't rely on this coin cell battery to remain installed at all times. Removing the battery will not cause any of these other settings to be lost because they are stored in flash memory.

So in summary, the ONLY setting affected by the removal of the coin cell battery is the boot-up time/date, after each power-up. And if it's resynced to an external time reference after the battery is reinstalled, the RTC is automatically corrected for future power-ups to have the approximately correct time/date.

---

## Shelf life for RTC battery

- Shelf life is how long the device can remain unused before placing into service
- Shelf life is 5 years, limited by an on-board replaceable battery (for BIOS). See info below.

**Email from Mark McGregor on 9/2/10:**



The SecureSync appliance contains one internal battery (A 3vdc -500mAh, Lithium coin cell battery, P/N BR3032). This battery is used as backup power to the ETX microprocessor (for functions such as saving the BIOS settings and for the RTC -yearReal Time Clock functionality, etc). The SecureSync battery is specified to operate over a wide temperature range of -30C to 80C.

The backup battery life is based on the current draw of the ETX module when the SecureSync power is off. Battery life= Battery capacity (A-hr)/battery current (A). The BR3032 capacity is 0.5 A-hr. The ETX draws 12.5 uA when off. This results in 4.57 years of backup time/off time. Battery is not drained when power is on.

For the 93xx (NetClocks), a CR2032 is used, 0.22A-Hr. It uses the same ETX with 12.5uA of current draw when off. This results in 2 years of backup time/off time for the 93xx, so the SecureSync is an improvement over the 93xx. The SecureSync battery is also specified to operate over a wider temperature range of -30C to 80C, whereas the 93xx is a -30C to 60C battery.

The battery is a socketed component, but changing of the battery needs to be performed at the factory, in order to reset the ETX BIOS settings once the battery has been replaced.

**Note:** Because the backup time/off time is a cumulative time, based on how the customer normally operates the equipment, we cannot put an exact "expiration time" on the battery. We can't just say the battery is good for 10 years, for example.

#### **Document for replacing the battery in SecureSync (P/N 1200-5000-0055) Refer to manuals in Released drive**

- **Also refer to:** [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement](#)

#### **Email from Dave Lorah to Masataka with TOYO (10/3/12)**

You are correct to think the battery has failed and isn't backing up the time. It could also be the time was not set properly when the BIOS was first configured or the ETX module was removed and the time not set after ETX was reinstalled. The default date for the ETX module is Jan 1, 2003.

If the battery has failed it could be due to a high current draw. I have seen this happen once where the battery was drained by a damaged capacitor C62. There also could be a problem anywhere in the path between the battery and the ETX module.

---

## **Aluminum capacitors in SecureSync**

**Q** Is there any aluminum capacitor in SecureSync?

**A reply from Dave Lorah (18 Jan 16)** The answer is yes, there are capacitors constructed with aluminum in the SecureSync. I am curious why the customer would want to know this?

## Compact Flash Cards (CF cards)



### Industrial grade Compact Flash card used in SecureSyncs/NetClock 9400s

- **MFG/Model:** SMART Modular Technologies/ DuraFlash™ XL+ CF 5.0 CF Card
  - **Our P/N:** MP20R-0004-1000 (in Arena): [https://app.bom.com/items/detail-sourcing?item\\_id=1202844920&version\\_id=10212771558](https://app.bom.com/items/detail-sourcing?item_id=1202844920&version_id=10212771558)
  - **CF card Capacity (from “Day one until at least March 2019):** 1GB
  - **MFG/Item Number “Smart Modular Technologies”** SS9FD01GH3B4IS01
    - **MFG Datasheet (online)** <https://www.smartm.com/product/xlplus-cf-50-cf-card>
- Contact info:
- **Mfg Datasheet: (in Arena):** [https://files.bom.com/download/qlsfMbl7nWQbX4BOM4quZwfDbzq8EEgW/omwrbcifkzfovqjxxwagzkynbqxifo/CF\\_Card\\_XL\\_XLplus\\_overview.pdf](https://files.bom.com/download/qlsfMbl7nWQbX4BOM4quZwfDbzq8EEgW/omwrbcifkzfovqjxxwagzkynbqxifo/CF_Card_XL_XLplus_overview.pdf)
  - [https://www.smartm.com/salesLiterature/removable/CF\\_Card\\_overview.pdf](https://www.smartm.com/salesLiterature/removable/CF_Card_overview.pdf)

| Specifications                           |                                                                                             | Ordering Information |                                  |          |
|------------------------------------------|---------------------------------------------------------------------------------------------|----------------------|----------------------------------|----------|
|                                          | CF Card XL                                                                                  | CF Card XL+          | Part Number                      | Capacity |
| <b>Performance</b>                       |                                                                                             |                      |                                  |          |
| Read (maximum)                           | up to 32MB/s                                                                                | up to 55MB/s         | 809CF128HYB1A                    | 128MB    |
| Write (maximum)                          | up to 16MB/s                                                                                | up to 27MB/s         | 809CF256HYB1A                    | 256MB    |
| <b>Reliability</b>                       |                                                                                             |                      |                                  |          |
| Data Reliability                         | 1 non-recoverable error in 10 <sup>14</sup> Bits, Read                                      |                      | 809CF512HYB2A                    | 512MB    |
| Data Retention                           | 10 years >90% life remaining<br>1 year at the end of life                                   |                      | 809CF10HYB4A                     | 1GB      |
| Endurance                                | CF Card XL: TBW = 5 Tbytes per 1GB capacity<br>CF Card XL+: TBW = 3 Tbytes per 1GB capacity |                      | 809CF20HYB6A                     | 2GB      |
| <b>Power</b>                             |                                                                                             |                      |                                  |          |
| VCC 5.0V (+10%)                          | 5.0V+10%                                                                                    | 3.3V+5%              | 809CF40HYB6A                     | 4GB      |
| Read                                     | < 200mA                                                                                     | < 200mA              | <b>CF XL (Industrial Grade)</b>  |          |
| Write                                    | < 200mA                                                                                     | < 200mA              | 809CF128HYDAI                    | 128MB    |
| Idle                                     | < 4mA                                                                                       | < 4mA                | 809CF256HYDAI                    | 256MB    |
| <b>Environmental</b>                     |                                                                                             |                      |                                  |          |
| Shock (operational)                      | 50G @ 11ms                                                                                  |                      | 809CF512HYDAI                    | 512MB    |
| Vibration                                | 15G peak to peak                                                                            |                      | 809CF10HYDAI                     | 1GB      |
| Operating Temperature - Commercial Grade | 0°C to 70°C                                                                                 |                      | 809CF20HYDAI                     | 2GB      |
| Operating Temperature - Industrial       | -40°C to +85°C                                                                              |                      | 809CF40HYDAI                     | 4GB      |
| Storage temperature                      | -50°C to +85°C                                                                              |                      | 809CF80HYDAI                     | 8GB      |
| Humidity                                 | 0% to 95%                                                                                   |                      | 809CF160HYDAI                    | 16GB     |
| Altitude                                 | up to 80,000 ft.                                                                            |                      | 809CF320HYDAI                    | 32GB     |
| <b>Physical</b>                          |                                                                                             |                      |                                  |          |
| Length                                   | 1.433 in. (36.40 mm.)                                                                       |                      | 809CF640HYDAI                    | 64GB     |
| Width                                    | 1.865 in. (42.80 mm.)                                                                       |                      | <b>CF XL+ (Industrial Grade)</b> |          |
| Thickness                                | 0.130 in. (3.30 mm.)                                                                        |                      | 809CF512HYDDI                    | 512MB    |
| Weight                                   | 0.36 oz. (10.2 gm)                                                                          |                      | 809CF10HYDDI                     | 1GB      |
|                                          |                                                                                             |                      | 809CF20HYDDI                     | 2GB      |
|                                          |                                                                                             |                      | 809CF40HYDDI                     | 4GB      |
|                                          |                                                                                             |                      | 809CF80HYDDI                     | 8GB      |
|                                          |                                                                                             |                      | 809CF160HYDDI                    | 16GB     |
|                                          |                                                                                             |                      | 809CF320HYDDI                    | 32GB     |
|                                          |                                                                                             |                      | 809CF640HYDDI                    | 64GB     |

Note: All available in industrial grade. 1GB not supported at this capacity.

- [https://www.smartm.com/salesLiterature/flash/SMART\\_Flash\\_products.pdf](https://www.smartm.com/salesLiterature/flash/SMART_Flash_products.pdf)

# Removable Flash Solutions

## CF CARD

DENSITIES FROM 128MB UP TO 64GB



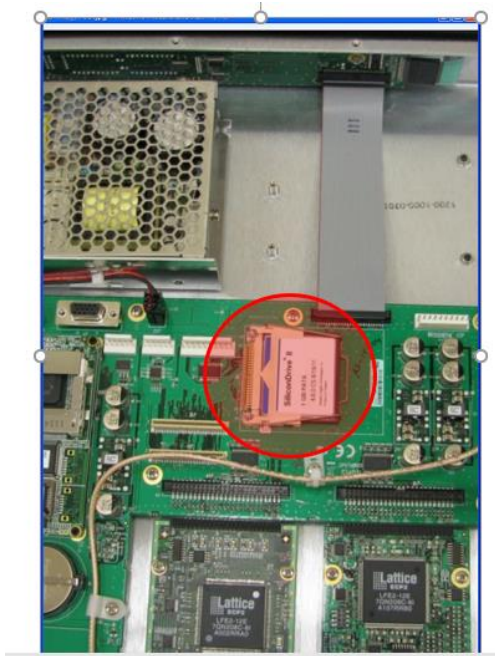
- Networking
- Telecom
- Embedded Designs

SMART's CF Cards are high-capacity, low-power memory cards that act like hard drives but are reliable, fast and portable. These cards also support self monitoring analysis and reporting technology (S.M.A.R.T.) attributes to help reduce unexpected field failures.

### Flash Card Products

|                 |               |                   |
|-----------------|---------------|-------------------|
| CF Card XL SLC  | 128MB to 8GB  | SS9FD08GH3BAxS01* |
| CF Card XL+ SLC | 512MB to 64GB | SG9CF64GHYDD*     |

\* Part number noted is that of highest density available



### Cage Code Number for CF Card

- Cage Code is 59797 (per Marlea Andolora 8 Oct 2019: As Denise mentioned, our cage code is **59797**)

### Individual serialization/identifiers for each CF card

- Refer to Salesforce Case 259336 (March 2021)

**Per Ron Dries (5 March 2021)** The CF cards do have manufacturer information, however this information is not accessible by the user.

### Specs/life expectancies (Rewrites/Erasing counts)

Questions below from TOYO / Responses from Stuart Burtner (14 Nov 2018) / Responses from Dave Sohn (15 Nov 2018)

1. Do you have any information about the limitation of the rewrite counts?

If I understand this question correctly, he's asking for an amount he can write to the disk before he'll exceed the erase count limitation. We don't have a very good figure for this because it depends heavily on how the disk is used.

Orolia has made improvements to provide ~10 years of operation before reaching the CF card specifications. Reaching the specification limit does not indicate that failure will occur, but failure rate may increase.

2. Do you have any information about the limitation of the erasing counts?

The information we have on erase count limitations is from the card's SMART data, which is as follows:

- **SMART will begin to report failure after ~370,000,000 erase counts** (with an estimate of 10% life remaining)
- **SMART will estimate 1% life remaining at 406,000,000 erase counts**

3. Do you have the MTBF?

Not at this time.  
> 4,374,870 hours

---

## CF card's Writes and Erases counter depleting

Versions 5.8.1 and below writing to the CF cards with too much data (resulting in them failing too early)

- Refer to CAPA-105 for details: [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CF cards \(compact flash\)\CF cards getting written to](..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CF cards (compact flash)\CF cards getting written to)
- Significantly improved in 5.8.2 update (~Oct 2018)
  - Per 5.8.2 Release Notes: "Improved data logging to prolong compact flash longevity"
- Expected CF card lifespan with v5.8.2 or above installed on a brand new card (not previously "partially used up") is about 10 years.

## Potential for files to become corrupt when the writes/erase counts has been depleted

Per Stuart Burtner (24 May 2021)

Our understanding is:

Any file on the system can become corrupt.

This is because the wear-leveling on the CF card will try to utilize sectors that are inhabited by existing files. It can move old files onto a bad sector, causing an existing file to become corrupt.

## Root Cause/fix

- Refer to CAPA-105 for details: [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CF cards \(compact flash\)\CF cards getting written to \(excerpt below\)](..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CF cards (compact flash)\CF cards getting written to (excerpt below))

## Root Cause Analysis

It was determined that a monitoring daemon was responsible for writing excessive amounts of data to the product's memory causing sectors in the CompactFlash card to go bad; potentially corrupting the file system.

To verify this theory, engineering set up a long-term test where several SecureSyncs were loaded with a program that was created to write as much data to the disk as possible. These units were monitored while under test until they failed and were unable to reboot. The disks were then evaluated for the cause of failure.

It was found that some disks were corrupt to the point of being unreadable and others had important files on the disk that were not useable.

The daemon responsible for performing these writes has been modified to substantially reduce its data throughput to the disk, increasing the longevity of the CompactFlash card. With the implemented changes, the CompactFlash card is expected to last at least 10 years, provided that available memory on the existing CF card is sufficient.

**email from Danny Loke (10 June 2021)** Toyo has asked me on the following questions on Skype and here's my reply:

Q1.What kind of writing is excessive writing? – it is the Monitoring Daemon in the Linux OS.

Q2-1.What is "a monitoring daemon"? – It is a computer program that monitors the various parameters of Securesync and it runs in the background during operation.

Q2-2How did you fix that daemon? – It is stated in the Root Cause Analysis and Correction Action of document CAPA-000105 1.

---

L3Harris customer advisory to replace installed CF card: **IPN 10.6.**

---

## Purchasing new CF cards for a unit outside of its 5 year warranty period

- See Denise Cond for info/assistance

**modified email from Jodi Campbell (14 Nov 2018)** Devices that are not under warranty would incur a fee of \$50.00 per CF card, plus a shipping fee of \$25.00 (per *shipment*, not per card). Or, we can instead use your shipping account number if you prefer, instead of the \$25.00 fee.

We do need to know the serial numbers and what version of software is running on the devices, first. I cannot send out sw version 5.8.2, blindly, unfortunately. If the software is too old for compatibility, it won't work with 5.8.2.

---

## Procedure to replace the CF card

Q Do you have a procedure that we can look at for the replacement? Other than just opening the box and looking for it to replace it. Also, if you have anything on the menus to configure the IP address from the front panel?

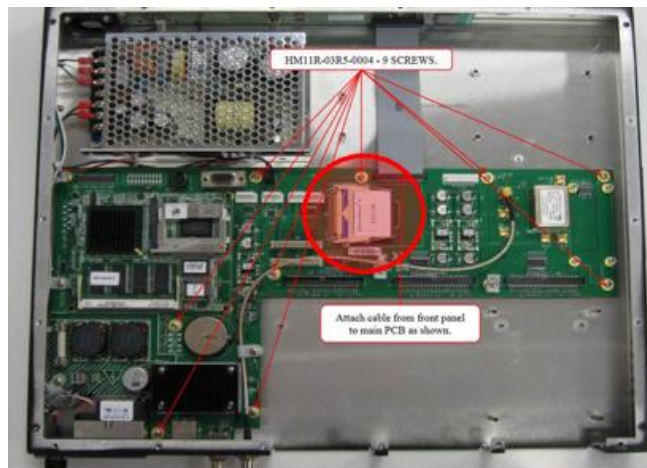
**A slightly modified reply from Dave L (19 Apr 17)** Yes, the procedure to replace the CF card is fairly simple.

**Note:** Make sure to follow standard ESD protection procedures.

1. Remove power from the device
2. Remove the device from the rack
3. Remove the top cover by removing the 20 Phillips head screws around the perimeter of the top cover
4. Remove the CF card by unfastening the wire clip that holds the card in a sliding the card out of the holder.

**Note:** Installation is the opposite of removal

Here is a photo of the PC Board inside the chassis (Please ignore the red lines to the screws). The CF card is in the center.



When the CF card is installed and the unit returned to the rack, power it on and wait a few minutes until the front panel indicates the network parameters. This will show eth0 by defaults and will pick up a DHCP address if one is available.

To set a static IP address to eth0, you first turn off DHCP and then enter the IP address. Here is a link to the Quickstart Guide which has good information on setting up the IP address using the front panel keypad.

<https://spectracom.com/sites/default/files/document-files/SecureSync%20QuickStart%20Guide%20PN1200-5000-0051Rev11.pdf>

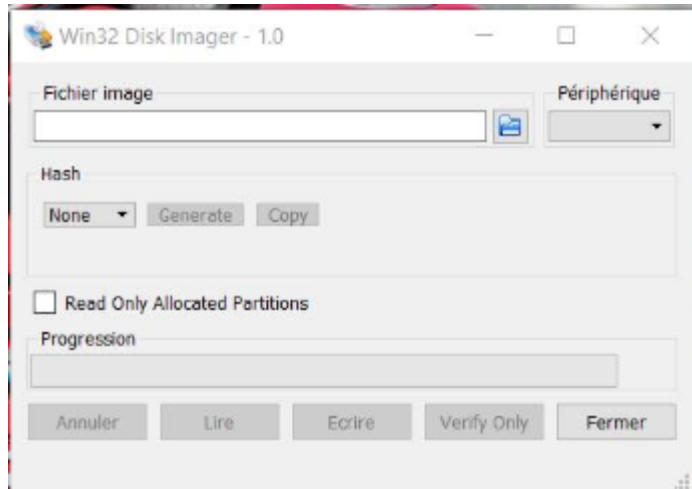
When the eth0 port is configured, you can then use the web Ui to enable and configure the other Ethernet ports or upload a saved configuration.

---

## Ability to burn new CF card image in the field/Replacing the CF card in the field

Per Eric Girard (24 Sept 2020) the freeware program below (**Win32 Disk Imager**) can be successfully burn the image file into customer-supplied 1GB CF cards.

➤ Refer to Salesforce Case 247557



### Email Dave L sent (regarding Salesforce Case 247557)

Not having done a manual CF card creation myself, I asked for guidance from a fellow support engineer.

He gave me this link you could use to download a known good image file for version 5.8.6. Once you have the unit up and running you should download the firmware update file and run the v5.8.9 update from our website and the entire system will be updated.

<https://files.spectracom.com/client-downloads/1463907735>

In the browser field, make sure that type is selected with \*.\* . If not, file won't be displayed.

The info in their GUI examples are in French, but here are some instructions:

From the software burner app, sorry it's in French, but I guess that it can be installed in English – Find your saved image file on your PC ( Fichier image ) , make sure of the right location of the CF ( Peripherique ) , do not burn your HDD laptop 😊😊😊- and then run the app ( Ecrire or write )

There is no option to confirm that the file has been copied properly like with a burner.

What I did to confirm this, I installed the CF in a SecureSync and I checked that the unit booted correctly and the right sw version was displayed.

Here is a link to get the latest version 5.8.9 firmware from our website if you do not have it already:

<https://files.spectracom.com/public-downloads/latest-securesync-netclock-files>

Q. Is it possible to burn/create a new CF card in the field

**A. Email from Dave L (18 Oct 2019)** We do not recommend programming your own CF card. The cards we use are high grade industrial quality Cf cards that are designed to meet our temperature specs. Also we produce each card on a CF card duplicator from a designated Master so each card is an exact clone of the master. This ensures all the firmware is in the same memory locations.

The firmware is available from our website if you would like to try your own but we would not be able to support this. Hopefully you will get the Cf card in a short time.

<https://files.spectracom.com/public-downloads/latest-securesync-netclock-files>

**A. Email from Dave L (20 Dec 16)** I cannot send the image for 5.4.5 because it does not work to write a card unless the exact memory locations are addressed. It is better to use a card copier to make new CF cards. We use a card copier and a Master CF card when we make CF cards here at Spectracom. This way each card is an exact copy of the master. If the card is not an

exact copy it may fail to run the Securesync properly

**A. An earlier email from Dave L (7 Dec 16)** The CF cards cannot be copied easily. You would need a card copier/duplicator that would copy the data to the exact locations on the new card. If the files are not in the same exact locations it will not work. We have a card duplicator here that works from a pre-programmed master CF card to make exact clones of the CF cards. I can program a CF card to ver 3.6.7 and send it to you free of charge. It is not worth returning the old CF card.

---

## CF card formatting/customer's desire to read/directly view the contents of a CF card

### In Windows

**Per Ron Dries:** "The card reader isn't the problem. The CF card uses a file system format that Windows does not support"

Q Is the CF card readable with Windows?

**A reply from Jodi (11 Feb 2019)** "The card is not formatted in Windows, but is written for Linux. A Linux box should be able to read the card, however."

---

## CF card write usage/expected life expectancy patch/software feature ("ss\_healthcheck\_v2.tar.gz" and "ss\_healthcheck.tar.gz")

- On our website: <https://files.spectracom.com/public-downloads/compact-flash-health-check-securesyncnetclock-9400>
- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\CF card healthcheck>
- In Arena ("1200-SU02-CFHC") at: [https://app.bom.com/items/detail-spec?item\\_id=1268530406&version\\_id=11637668668&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1268530406&version_id=11637668668&orb_msg_single_search_p=1)
- three different file versions (first version didn't support v5.8.4 variants such as 5.8.G, second version didn't support 5.8P)
  - `ss\_healthcheck.tar.gz` can only be applied to versions 5.1.2 through 5.8.4
  - `ss\_healthcehck\_v2.tar.gz` (added support for version 5.8.D, 5.8.E, 5.8.G, and 5.8.J) can be applied to versions 5.1.2 – 5.8.4, along with 5.8.D, 5.8.E, 5.8.G, and 5.8.J.
  - `ss\_healthcehck\_v3.tar.gz` (added support for v5.8P) can be applied to versions 5.1.2 – 5.8.4, along with 5.8.D, 5.8.E, 5.8.G, 5.8.J and 5.8.P
- After installing the free basic patch (or in versions 5.8.5 and above) the CF card's life expectancy is reported at the bottom-left of the **Tools** -> **Upgrade/Backup** page of its browser.
- Note the patch persists reboots, but does not persist software updates.
- Version 5.8.5 added this capability as a standard function (so this patch is no longer necessary when updating to versions 5.8.5 or above)
  - Per 5.8.5 Release Notes: "Added a Disk Healthcheck feature to the Web UI under **TOOLS** > **Upgrade/Backup**, which reports the approximate remaining life of the CF card and provides instruction to take action if necessary."

(As also excerpted below) For the associated details, refer to **Section 2.2** of the document at: [https://files.spectracom.com/sites/default/files/public\\_files/1557283959/thcheckReleaseNotes.pdf/](https://files.spectracom.com/sites/default/files/public_files/1557283959/thcheckReleaseNotes.pdf/)

## 2.2. Results

To view your Disk Healthcheck results:

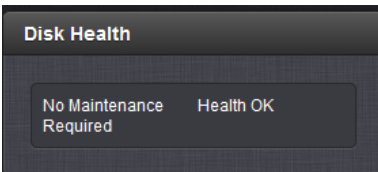


- After installing the software patch, refresh the Upgrade/Backup page.
- A new Disk Health panel will display (below Disk Status). This information will update daily.
- Your Disk Status will either be **Disk Maintenance Required** or **No Disk Maintenance Required**. A status of Disk Maintenance Required will include an approximate length of life in months.
- If your Disk Health is **more than approximately three months**, your unit will have enough disk life to upgrade to the latest version of the software. (Upgrade is strongly recommended to preserve your disk).
- If your Disk Healthcheck estimates **less than three months**, do not upgrade your unit. Contact Customer Support.
- See contact information below for additional information on your projected disk life.

### “Disk Health”: Checking CF card health status

#### A) via web browser (*Tools* -> *System Monitor* page)

(Left- side of page, towards the bottom)



“**No Maintenance Required Health OK**” indicates that the CF card has at least three months remaining, before needing to be replaced.

#### B) Via REST API

#### C) Available CLI command to check health (instead of having to view it in the browser/using REST API)

- Believe this this command is available in **v5.8.5** and above.
- Type: **healthcheck.sh**<enter>

```
spadmin@Spectracom ~ $ healthcheck.sh
Nov 08 21:50:43 Spectracom Spectracom: [health] Disk Health OK - No maintenanc
required (166826896)
spadmin@Spectracom ~ $
```

“**Disk Health OK - No Maintenance Required.**” indicates that the CF card has at least three months remaining, before needing to be replaced.

**Per Ron Dries (8 Nov 2019)** “I found out a customer can issue the command “**healthcheck.sh**” from the cli and it will return the status.”

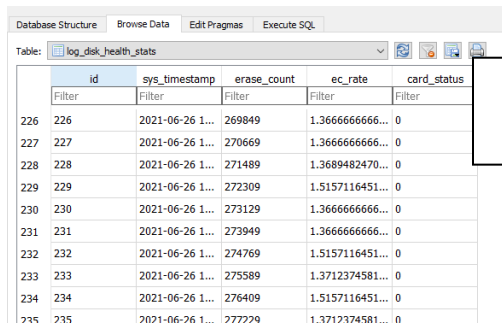
**Status update (per Keith 28 April 2023)** I tried this command on the v5.9.6 beta software and it didn’t respond correctly. Not sure if this was due to the convergence build (just affecting the beta) or this command may have stopped working in a previous version (possibly due to the Write counts now being stored in the sqlite database perhaps??)



## D) Via System logs\_status

### 1. "log\_disk\_health\_stats" data in the sqlite dbase (newer versions such as 5.8.9 and above)

**Note:** Apparently, with newer versions such as 5.8.9 and above, diskhealth.log info is now in the sqlite database, instead of a separate diskhealth.logfile in the log bundle (see below):



| id  | sys_timestamp   | erase_count | ec_rate          | card_status |
|-----|-----------------|-------------|------------------|-------------|
| 226 | 2021-06-26 1... | 269849      | 1.36666666666... | 0           |
| 227 | 2021-06-26 1... | 270669      | 1.36666666666... | 0           |
| 228 | 2021-06-26 1... | 271489      | 1.3689482470...  | 0           |
| 229 | 2021-06-26 1... | 272309      | 1.5157116451...  | 0           |
| 230 | 2021-06-26 1... | 273129      | 1.36666666666... | 0           |
| 231 | 2021-06-26 1... | 273949      | 1.36666666666... | 0           |
| 232 | 2021-06-26 1... | 274769      | 1.5157116451...  | 0           |
| 233 | 2021-06-26 1... | 275589      | 1.3712374581...  | 0           |
| 234 | 2021-06-26 1... | 276409      | 1.5157116451...  | 0           |
| 235 | 2021-06-26 1... | 277229      | 1.3712374581...  | 0           |

**"Card Status"**  
0 = No Maintenance required (CF card OK)  
1 = Disk Maintenance required (CF needs to be replaced)

**EC: Erase Counts go UP (not down) (per Stuart, 400 million is 1% remaining)**

[1:00 PM] Stuart Burtner

- **Yep 400 million is when it reaches "<1% life remaining"**

[1:00 PM] Stuart Burtner

- **360m is the "<10% life remaining"** which is the beginning of the warning

[1:00 PM] Stuart Burtner

(From the manufacturer, not from our side. I don't remember what our timeframes are calibrated around - likely the 10% mark)

[1:01 PM] Stuart Burtner

and IIRC, EC\_Rate is in **erase counts per second**.

### A) dischealth.log (contained within log bundle) (earlier versions such as versions 5.8.8? and below)

- Healthcheck is performed once-per-day at UTC midnight
- Results are logged

- Example: "Jun 03 00:00:00: [health] Disk Health OK - No maintenance required (969647)"

### "Acceptable" Life expectancy remaining before SAFELY applying a software update

- Per Scott Z and Stuart, a **GOOD** estimated "life remaining" to safely apply a software update to a newer version (to have the unit crash/die during the update process) is **3 months or greater**
- If a CF card is reported to have **less than 3 months** remaining, a successful software update cannot be assured, so the CF card should therefore be replaced before applying a software update.

### If an "original" (Western Digital - WD) CF card happens to be installed

\$ **healthcheck.sh**

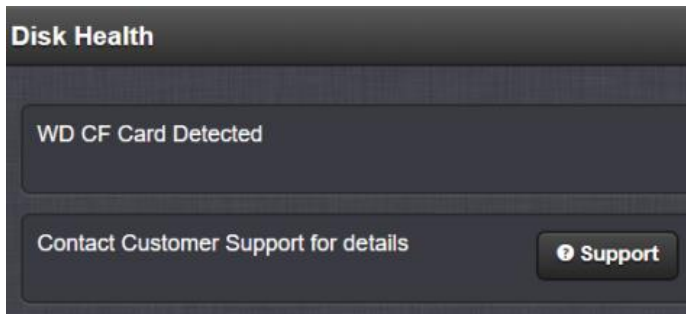
Jun 09 14:38:35 slcicntp02 slcicntp02: [health] Failed to determine health of disk - WD CF Card Detected (4)

- Patch/healthcheck update is not compatible with the original Western Digital CF Cards

➤ If a Western Digital card is installed, patch just reports “**WD CF Card Detected**”)

- WD Card should automatically be replaced

**example reply from Dave L (17 Jan 2020)** If you have a older Seuresync it may have a CF card from a different vendor (WD = Western Digital) and the card does not have the capability to read the number of read/write cycles. If you see any Seuresyncs with the WD cards, these are old and should be replaced.



**Email Keith sent to Nidal (14 May 2019)** Scott Z had mentioned to us that the patch is compatible with software versions 5.1.2 and higher (the patch needs the newer black/charcoal background which was added in version 5.1.2).

But he also mentioned that original (VERY early) SecureSyncs shipped with a different type CF card (Western Digital card - not the “smart cards” we have been using since switching a long time ago).

These early model “WD” CF cards, even if the software has since been updated to version 5.1.2 or above, are not compatible with the health patch. Since the patch can’t ascertain the “read/erase” numbers of these earlier model CF cards, the patch just reports the CF card was detected, without being able to report its expected remaining “life”...

---

## \*\*Grub errors/indications of a failing CF card

- Per Paul Myers, grub errors are due to file system corruption.
- Seem to happen during a power cycle to units that have been fielded for a couple of years
- If the unit is still in the field, send a new CF card programmed with the same version as the fielded unit.

### What is Grub

Per Paul M, Grub is the “bootloader” program/software used to initially load the Linux OS in the CF at each boot-up

Below is from <https://askubuntu.com/questions/347203/what-exactly-is-grub>

Basically, GRUB bootloader is the software that loads the Linux kernel. (It has other uses as well). It is the first software that starts at a system boot.

When the computer starts, BIOS first run a Power-on self-test (POST) to check hardware like memory, disk drives and that it works properly.

Then BIOS checks the Master Boot Record (MBR), which is a 512 byte section located first on the Hard Drive. It looks for a bootloader (like GRUB). The hard drive’s partition tables are also located here.

Then you’ll be prompted by the GRUB menu which can contain a list of the operating systems installed, or perhaps the different kernels installed in a Linux distro.

When you choose which distro or kernel you want to use, GRUB loads the selected kernel. The kernel starts init (or systemd), which is the first process to start in Linux. Init then starts other processes like network services and other that you might have configured to start at boot time.

List of GRUB error numbers and causes: [https://wiki.gentoo.org/wiki/GRUB\\_Error\\_Reference](https://wiki.gentoo.org/wiki/GRUB_Error_Reference)

To see indications of a failing/bad card, review the kernel log for “hda” entries such as:

```
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=1583721, sector=1583721
```

```

Mar 23 14:55:34 Spectracom kernel: hda: possibly failed opcode: 0xc8
Mar 23 14:55:34 Spectracom kernel: blk_update_request: I/O error, dev hda, sector 1583721
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=1583721,
sector=1583721
Mar 23 14:55:34 Spectracom kernel: hda: possibly failed opcode: 0xc8
Mar 23 14:55:34 Spectracom kernel: blk_update_request: I/O error, dev hda, sector 1583721
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=1583721,
sector=1583721
Mar 23 14:55:34 Spectracom kernel: hda: possibly failed opcode: 0xc8
Mar 23 14:55:34 Spectracom kernel: blk_update_request: I/O error, dev hda, sector 1583721
Mar 23 14:55:44 Spectracom kernel: spurious 8259A interrupt: IRQ7.

```

**Another example Email from a customer (3 Jan 18) For example, some errors look like "ata1.00: failed command: READ DMA", and "blk\_update\_request: I/O error, dev sda, sector 279169". The blk\_update\_request error happens often and it is always sector 279169.**

## “NTLDR is missing. Press any key to continue” error

- Refer to SF case 120331

**Q Report from Customer** ...And lastly I would like to report a finding which I find it unusual.

You have sent me two identical 5.1.4 CF Cards. But only one of the card is working fine, the other card shows the same “NTLDR is missing” error ; which is the same error for the two 5.3.0 CF Cards that you sent me earlier.

```

CPU Type: Pentium III
CPU Frequency: 500MHz
CPU Processor: Pentium III
CPU Cache: 256KB
Cache Memory: 128K
Diskette Drive A: None
Diskette Drive B: None
Pri. Master Disk: CHS, 676 33, 1025MB
Pri. Slave Disk: None
Display Type: VGA-960
Serial Port(s): 370 270
Parallel Port(s): 270
SMBus at I/Os: 0

PCI Device Listing ...
Bus No. Device No. Func No. Vendor/Device Class Device Class
0 1 1 1022 2081 0300 Display Contrlr
0 1 2 1022 2082 1010 En/Decryption Contrlr
0 6 0 10EC 8139 0200 Network Contrlr
0 9 0 1AB7 8900 0500 Memory Controller
0 15 2 1022 2090 0101 IDE Contrlr
0 15 4 1022 2094 0C03 USB 1.0/1.1 OHCI Contrlr
0 15 5 1022 2095 0C03 USB 2.0 EHCI Contrlr

NTLDR is missing
Press any key to restart

```

I just want to let you know about this peculiar finding, you do not have to send me a replacement.

**From:** <https://www.lifewire.com/how-to-fix-ntldr-is-missing-errors-2623859>

### Typical Causes of NTLDR Errors

There are a number of possible causes for [NTLDR](#) errors, including the most common "NTLDR is missing" issue.

The most common reason for this error is when your computer is trying to [boot](#) from a [hard drive](#) or [flash drive](#) that is [not properly configured to be booted from](#). In other words, it's trying to boot from a *non-bootable* source. This also would apply to media on an [optical drive](#) or [floppy drive](#) that you're trying to boot from.

Other possible causes include corrupt and misconfigured files, hard drive and [operating system](#) upgrade issues, corrupt hard drive [sectors](#), an outdated [BIOS](#), and damaged or loose [IDE cables](#).

---

### \*\*\*Sending a replacement CF card to a customer/replacing CF card in the field

➤ refer to [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CF cards \(compact flash\)\](..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CF cards (compact flash)\)

#### International shipping paperwork (ECCN and HTS code) for the **CF card**

- **ECCN:** EAR99
- **HTS code:** 8523.51.0000
- **Country of Origin (COO):** Malaysia (MY)

#### Cost/value of the CF card

Per [Laura C \(21 Feb 2023\)](#): \$22.00

**Much earlier Email from Linda M to Mary Slack (8 Apr 2016)** I checked with Sara, our cost is \$21.25/ea from the supplier and the standard cost is \$21.67. Please let me know which value should be used for the CI.

---

### How to tell if the CF card has been replaced

Q How can we verify if the CF card has been replaced in the past?

**A Reply from Dave L (26 May 2021)** The best way to verify the CF card has indeed been replaced is by opening up the chassis and looking at the Date and Version label on the CF card itself.

Checking the CF card via the web UI or Command line is possible.

This is more difficult because these Securesyncs are running an older version 5.8.P firmware that did not have the Disc Health Check Utility added yet. The Disc Health Check will determine the health of the CF card based on the number of erase cycles recorded on the card and calculate the expected remaining functional life of the CF card. We do have a patch that can be installed on the Securesync, in the same manner as a firmware update, that will add this feature to the Securesync. After installing the Utility the Disc Health should indicate the CF card needs replacing if these units are in need of CF card replacements.

Installing this patch will not reboot or interrupt the Securesyncs operation.

Here is a link to our website to download the Disc Health Check Utility and instructions:

[Compact Flash Health Check for SecureSync/NetClock 9400 | Spectracom Fileshare](#)

---

### Sending a replacement Compact Flash (CF) card to install in units still at much older versions, such as 4.8.7 to 4.8.9 (will KTS be updated by the much newer version updater process??)

**Per Ron Dries (5 Feb 2020)** I don't remember testing this in a while, but it should be OK.

The step updating was mainly for the NWP as there were significant changes made between 4.8.X and the 5.X.X.

They may need to do the upgrade from the CLI as there are some significant changes in KTS between 5.8.6 and 4.8.9.

**Per Morgan Randolph (5 Feb 2020)** I tested this process at v4.8.9 and it should work, I did not try below that version. You should be able to send the card and run the installer.

---

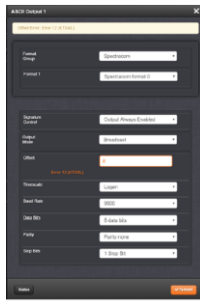
### After replacing a CF card in the field, customers still need to perform update process- to update KTS to the correct corresponding version

#### Example symptoms of KTS not yet being updated to the correct version

#### 1. **“Offset Error: Error 12 (KTSAL)”** message reported while trying to configure ASCII output

- Refer to Case 196586
- Replacement Card was at v5.8.4 and KTS hadn't been updated yet (unit was previously at 5.8.1?)
- caused by a new “Offset” field being added in a more recent version than what was previously installed

- fixed once the version 5.8.4 upgrade was performed with a force upgrade.



### If Opt-BSH BroadShield option is enabled, when replacing the CF card

- Swapping out CF card apparently removes Opt-BSH option.

*Below is a sample email Dave Lorah sent to a customer (24 Nov 2020) Opt-BSH info is in bold*

Attached is an instruction on how to replace the CF card.

Once the CF card has been installed and you have the unit up and running again please run the v5.8.9 firmware upgrade process as outlined in the instructions to finish the firmware upgrade on the entire system. It is very important to run the update after the CF card has been installed as other portions of the system require upgrade as well.

The v5.8.9 update file is already be loaded on the CF card.

Also, our records indicate the Option BSH is installed on this serial number 20046.

Here is a link to download the Broadshield Firmware patch. This can be loaded into your SecureSync the same way a firmware update is done. Please note this download is only good until December 26.

<https://files.spectracom.com/client-downloads/173116283>

The file needs to be unzipped/decrypted using the password: Fz5J@esJ5i@R

This is an encrypted zip file. To install Broadshield to the system, follow these steps:

1. decrypt/unzip the file 'broadshield\_encrypted.zip' using the password mentioned above. The resulting file will be '1200-SU02-B522.tar.gz'
2. within the SecureSync WebUI, upload and apply the 1200-SU02-B522.tar.gz file per the standard update process

You may receive an error during the installation:

In: failed to create symbolic link '/etc/runlevels/default/broadshield': File exists

Oct 27 20:53:55 Spectracom Spectracom: [spupdate] Hot Patch 5.8.9 X.X.X Failed (SWUE)

Oct 27 20:53:55 Spectracom Spectracom: [spupdate] Problem applying hot patch! (SWUE)

Error while performing upgrade!

Exit: call to updater failed

This is OK and the Broadshield software package will be installed. Please check the web UI to make sure it has installed properly.

If you ever need to perform firmware updates in the future, here is a link to get the most current firmware version, instructions and release notes from our website.

<https://files.spectracom.com/public-downloads/latest-securesync-netclock-files>

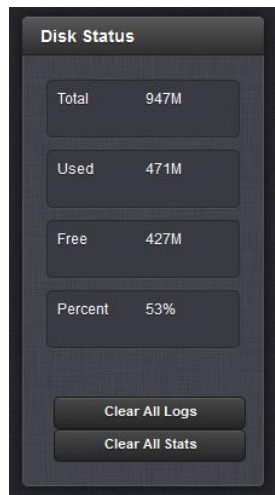
If you have any questions or need assistance please let me know.

---

## Report of CF card/Memory status

- Update version 5.2.0 added CF card memory status to the newer web browser (not available in classic interface). Also added ability to delete logs and Statistics from the same location

- **Tools -> Upgrade/Backup** page of the browser



---

## RTC (Real Time Clock) / Linux kernel time

### Linux Kernel time (summary of time at each start-up)

- When the SecureSync is powered down, the RTC gets its battery power from the ETX coin cell battery.
- The coin cell battery doesn't allow RTC to store the time. The battery just allows the RTC to keep incrementing the time while input power is removed.
- Refer to Mantis case 0001704 for more info:
- The battery-backed Real Time Clock (RTC) is read upon each boot-up in order to set the Linux kernel time.
- The kernel time then sets the KTS time.
- The kernel time is adjusted by NTP during synchronization to other references.
- Fcron (scheduler program) runs every 10 minutes to write the linux time to the RTC.
- Upon a Reboot or halt being performed, the kernel time is set into the RTC.

**Note:** If the time is manually set, KTS is set to this time. If the time is set backwards by any amount, Fcron may stop running until time catches up, and therefore it may not set the RTC. If the unit is then power cycled (not Rebooted or Halted), the manual set time is lost upon reboot. In order for the manual set time to be retained for the next power-up, a Reboot or Halt needs to be performed.

Update: this issue was fixed in the version 5.0.0 software update. Refer to Mantis case 2091 (<http://cvsmantis.int.rolia.com/mantis/view.php?id=2091>)

**Note:** the TSync-PCIe boards do not have an RTC, so this info does not apply to the timing boards.

---

## Sample log entries associated with RTC (note there may be others, also)

### From cron.log

Time saved to RTC (should be logged every 10 minutes:  
fcron[3565]: Job /etc/init.d/Cronhwclock save started for user root (pid 3566)

### From kern.log

After system reboot: rtc\_cmos rtc\_cmos: setting system clock to 2014-09-09 22:15:57 UTC (1410300957)

## RTC “accuracies” while SecureSync is powered down

- The BEST that the BIOS can set the SecureSync’s time at start-up is 0.5 seconds (it sets the time to the closest ½ second)
- The RTC uses a very low quality oscillator to maintain the time. This time will inherently drift off of the correct time, the longer that SecureSync is powered-down (the BIOS time is updated when the SecureSync powers down, but it then drifts from there).
- We do not currently have any specs for the drift of the RTC (when power is not applied) see email below from Tom.

SecureSync RTC drift can't be predicted because the RTC is on the ETX single board computer. Spectracom does not know what the RTC/crystal is on the ETX. An inquiry could be made to the ETX board manufacturer, Advantech about RTC time drift during power loss. It also depends on the RTC crystal and environmental conditions, change of temperature, etc. I do not know the SecureSync software, but I think the ETX time, NTP and RTC time, is updated from KTS timing system when the unit achieves synchronization. I do not know how often this time is refreshed.

There are no specifications given for the RTC because it is provided for “coarse maintenance” of the time base when a SecureSync that was in Sync powers off. The idea is that the date will be correct, and the time will be “close” to correct when power is restored, which is better than starting up and waiting up to 12 minutes for GPS to become in sync to get time and date. I do not believe it was ever intended for the customer to depend on the RTC time accuracy/drift over a power outage. It is outside the scope of the product specifications/requirements.

In order to answer this persons RTC question an inquiry to Advantech should be made, or maybe a SecureSync could be tested to get a typical value for room ambient temperature, but I don't know the resolution of the time a user can get from the system or what methods the user has available to get the time from the system. Maybe a software guy or Ron might know this information

FYI – The Rb does not get time or keep time, ever. The Rb disciplines its 10MHz output to a 1PPS reference. The Rb 10 MHz is the input to the KTS hardware clock. KTS hardware clock is what loads time from the RTC at power up and keeps time. This time will be updated when the unit again achieves time sync, at that point the RTC time is over written in KTS and the KTS time is sent to the ETX to update the RTC as well. After a power cycle the RB has to go through warm up of about 7 minutes before the Rb 10 MHz is good enough to use.

Q I the user reference guide "Document Part No.: 1200-5000-0050 Revision: 25 Date: 28-Aug-2017" there are references to a battery backed internal Real Time clock, but no specifications on the accuracy of this clock. On page 151, it states:

"The Accuracy of the Battery Backed Time depends on the accuracy of the hand-set time if the time is set manually in an autonomous system. In a non-autonomous system (i.e, when using external reference(s)) SecureSync's System lock will regularly update the battery-backed time. Another factor impacting the accuracy of the battery-backed time is how long a SecureSync unit is powered off: Any significant amount of time will cause the battery-backed RTC to drift, i.e. the battery-backed time will become increasingly inaccurate. The battery used for the RTC is designed to last for the lifetime of the product."

I am interested in the case where the unit is operating, receiving GPS time, and keeping the real time clock updated. Then, power is lost, recovers a few hours later, and GPS is no longer available. (At that point I expect the Rb standard starts and loads from the Real Time Clock.)

I need to know the accuracy of the real time clock so I can calculate how much drift might occur if the unit lost power and GPS was not available when repowered a few hours later. I am looking to achieve and project accuracy down to milliseconds levels

- A. Reply from Mark McGregor (7 Feb 8)** SecureSync RTC drift can't be predicted because the RTC is on the ETX single board computer. Spectracom does not know what the RTC/crystal is on the ETX. An inquiry could be made to the ETX board manufacturer, Advantech about RTC time drift during power loss. It also depends on the RTC crystal and environmental conditions, change of temperature, etc. I do not know the SecureSync software, but I think the ETX time, NTP and RTC time, is updated from KTS timing system when the unit achieves synchronization. I do not know how often this time is refreshed. There are no specifications given for the RTC because it is provided for “coarse maintenance” of the time base when a SecureSync that was in Sync powers off. The idea is that the date will be correct, and the time will be “close” to correct when power is restored, which is better than starting up and waiting up to 12 minutes for GPS to become in sync to get time and date. I do not believe it was ever intended for the customer to depend on the RTC time accuracy/drift over a power outage. It is outside the scope of the product specifications/requirements.

In order to answer this persons RTC question an inquiry to Advantech should be made, or maybe a SecureSync could be tested to get a typical value for room ambient temperature, but I don't know the resolution of the time a user can get from the system or what methods the user has available to get the time from the system. Maybe a software guy or Ron might know this information

FYI – The Rb does not get time or keep time, ever. The Rb disciplines its 10MHz output to a 1PPS reference. The Rb 10 MHz is the input to the KTS hardware clock. KTS hardware clock is what loads time from the RTC at power up and keeps time. This time will be updated when the unit again achieves time sync, at that point the RTC time is over written in KTS and the KTS time is sent to the ETX to update the RTC as well. After a power cycle the RB has to go through warm up of about 7 minutes before the Rb 10 MHz is good enough to use.

**Email from Tom Richardson (20 Dec 2012)**

AMD CS 5536 companion chip.

32 KHz Input. This input is used for the real-time clock (RTC), GPIOs, MFGPTs, and power management functions. This input may come from either an external oscillator or one side of a 32.768 KHz crystal. If an external oscillator is used, it should be powered by VIO\_VSB. This signal takes approximately one second to lock after power-up.



I found a crystal on the board looks something like this. Marked "C3N7C". Can't find any specs but it probably isn't worse than 100 PPM.

100 ppm x 24 hours is 8 seconds.

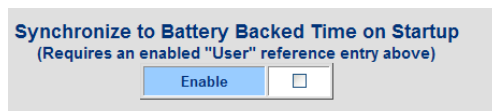
25 ppm for 24 hours is about 2 seconds.

0.5 seconds in 24 hours is 5 ppm

I took a quick look at Digikey and they have 20 ppm stock, about 1.7 seconds per day.

As in anything your mileage may vary.

**Keith's email to TOYO (20 Dec 12):** Yes. The SecureSync does maintain an estimate of the current time/date while the SecureSync is powered down. This is to allow the approximated time/date to be displayed at start-up (or starting in Archive software version 4.8.0, SecureSync can be configured to use this time/date for its initial synchronization, even though it's not very accurate. This is configured by enabling the "Battery backed Time" checkbox on the Setup -> Reference Priority page of the browser, as shown below).



The time/date during equipment power-down is not maintained by the SecureSync's 10MHz oscillator (which is not operational without input power applied to the SecureSync). Instead, the start-up time is simply maintained by the Real Time Clock (RTC) inside the system's ETX embedded CPU module. This RTC is powered by the internal coin cell battery and estimates the start-up time/date to within no better than 0.5 seconds of the actual time (this 0.5 second time error does not account for inherent oscillator drift- only the ability for the time to be set at start-up. Inherent drift of the RTC while power is removed will affect the overall accuracy of this time).

The RTC in the ETX module uses a very low quality oscillator to maintain the BIOS time while the SecureSync is powered-down. As this crystal is inherently not very stable, the RTC time will continue to drift off of the correct time, the longer the SecureSync is powered down. We do not have any specifications on the time drift. However, if its desired to maintain the SecureSyncs time as accurately as possible, the SecureSync should be operated with an uninterruptable power source (UPS), in order to prevent the SecureSync from being powered-down (and therefore, the SecureSync's time can be maintained by GPS, instead of via the RTC clock).

To prevent the chance of inaccurate time at startup from being used by external devices for their synchronization, the "Synchronize to Battery Backed Time on Startup" checkbox in the **Setup -> Reference Priority** page should not be enabled (it is not checked by factory default), if the "User" reference is enabled in the Reference Priority table. With this checkbox not enabled, the SecureSync will not automatically use the RTC clock as a time reference for its synchronization (manual intervention via the web browser is required after each boot-up, before the RTC time can be used for SecureSync's synchronization (thereby allowing a user to be



able to update the SecureSync's startup time, before it can declare sync using the BIOS backed time).

### 500ms error in versions 4.8.5 and below (fixed in v4.8.6)

#### Email from Paul Myers (2/28/12)

Note on reboot after an update the time is exactly 500 msec off. The RTC estimates to within a half second.

| Sync | Host         | Ref ID       | Stratum | LI | Mode   | Type    | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|--------------|--------------|---------|----|--------|---------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| ..   | System Time  | .LOCL.       | 16      | 00 | Client | local   | none        | 0          | 16                  | 0     | 0.000      | 0.000       | 4000.000    |
| **   | System PPS   | .PPS.        | 0       | 11 | Client | local   | none        | 0          | 16                  | 0     | 0.000      | 0.000       | 4000.000    |
| **   | 127.127.1.0  | LOCAL(0)     | 15      | 00 | Client | local   | none        | 1          | 16                  | 377   | 0.000      | 0.000       | 0.001       |
| **   | 96.9.150.154 | 128.118.25.5 | 2       | 00 | Client | unicast | none        | 15         | 64                  | 37    | 29.905     | 500.000     | 2.836       |

**Note:** 127.127.1.0 in the table above is the local system clock (the kernel time, as set by the RTC at power-up) The RTC error that Paul was referring to in his email above is the time difference between 127.127.1.0 and an external reference (in this case NTP server 96.9.150.154) the time difference is 500 ms (in the offset field).

### RTC being set when manually setting the System time backwards into the past

- When System Time is advanced into the future, RTC is updated every 10 minutes.
- When System Time is set back into the past, RTC isn't updated the first time for about 3 to 4 hours. Then it's updated every 10 minutes again.

The system is not intended to be a simulator. It especially does not like being set backwards to an earlier time. This causes Cron to completely stop running, until time has caught up to the correct time.

If the time is set backwards and then power cycled without a several minute delay, it will not power-up with the time that it was manually set to. It takes several minutes for NTP to change the kernel time, once it's been manually set. Then Cron, which is used to periodically set the RTC stops running until time catches up to the kernel time. If the time is set backwards, a delay of several minutes (like 20 to 30 minutes) should occur between setting the time and power cycling the unit.

**Email Keith sent to Masataka (18 Feb 15)** Thanks for your email. Our Applications Engineering team has reviewed the information you provided us with regards to the SecureSync's RTC being saved. I am happy to pass along to you their findings.

To begin, when manually setting the time of the SecureSync, there is a one particular scenario that will allow the RTC to be automatically saved within 10 minutes of setting the time. There is another scenario which prevents the System Time from being able to be automatically saved to the RTC for a few hours, unless a reboot or halt of the SecureSync is commanded.

If the System Time/date is manually set by a user to a time/date ahead of the current System Time, the SecureSync continues to be able to automatically set the time into the RTC every 10 minutes (on a 10 minute schedule). However, if a user manually sets the date/time to an earlier date/time than the System Time was set to, the System Time can't be automatically set into the RTC for about 3 to 4 hours, unless a *reboot* or *halt* command is performed.

If the date/time is set by a user to a date/time in the past and its desired to save this "new" date/time into the RTC without waiting the 3 to 4 hours for it to be automatically saved, the SecureSync should be commanded to be either rebooted or halted (not just power cycled) after setting the date/time backwards. Note the RTC is not updated upon a power cycle of the SecureSync. However, the RTC is updated with the System Time upon either a reboot or a halt command being issued. The SecureSync can be either rebooted or halted via the front panel menus, the web browser, the CLI command line interface or via SNMP.

Please be aware that the RTC taking a few hours to be set when a user sets the date/time into the past is not a software bug and Spectracom has no intentions at this time of changing how this operates. If it's desired to manually set the time of the SecureSync backwards to a previous date/time for some reason, the SecureSync should be either rebooted or halted (via its user interfaces) in order to alleviate the need to wait the 3 to 4 hours that is needed for the RTC to be updated with this earlier System Time. Note

that the RTC is updated with each reboot or halt command, whether the date/time was set forward or backwards from the starting System Time. The reboot/halt command alleviates any need to wait for the RTC to be updated, as the RTC update occurs before the SecureSync is brought down with either command being performed.

---

## Site acceptance testing / performance testing

- Refer to: <\\Rocfnp01\drivedata\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\Acceptance tests>

---

## SecureSync Options

### Options/License files available for SecureSync (besides Option Cards)

- Refer to the SecureSync datasheet: [I:\Marketing\Product Data Sheets \(archive\)\Time & Frequency References](I:\Marketing\Product Data Sheets (archive)\Time & Frequency References)

---

### Generating/installing license files

#### SecureSync License Bundle Creator

- refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\License Files Updates>

**Per Ron Dries (25 Jan 18)** The updated License creator tool is being kept in Arena.

The item number for the tool is SS\_LIC\_PROG\_CS. It can be found here: [https://app.bom.com/items/detail-spec?item\\_id=1242672189&version\\_id=10893367128&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1242672189&version_id=10893367128&orb_msg_single_search_p=1)

It can be run by downloading it to your PC and extracting it. The executable is called **bundleCreator.exe**.

Enter the model and serial number into the GUI and then check the licenses you would like to include in the bundle for the specified model and serial number.

After pressing submit the file is created in the directory C:\ManufacturingProgrammingFiles\ on your PC.

**Associated response from Dave L:** I have placed the new update file in I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Software Update- license files. I have also updated the license file creation instruction to reflect this new procedure.

---

### Installing licenses

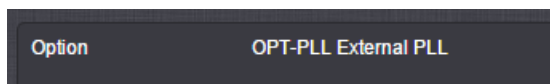
- Specific process to install license can vary based on installed software version.
  - For example, version 5.2.1 has a dedicated button to upgrade License File (installing license is not the same process as updating the software)

#### Process for updating a SecureSync\NetClock customer unit in the field (email from Tom Richardson)

- 1) Sales/Customer service gets order for update license from customer. Customer supplies required serial number(s).
- 2) Order Entry enters order and adds serial number(s) as a line note. Notifies Customer Service.
- 3) Customer Service creates license update file following the license file creation process.
- 4) License file and installation instructions sent to Customer through Salesforce.
- 5) Unit notes in Salesforce are updated to reflect serial number change in status.
- 6) Customer service notifies Operations that item has shipped and Shipping update transaction in Visual.

### Browser report of installed license files

- The license status is visible on the TOOLS -> Upgrade/Backup page in the web user interface. It should be listed under the "System Configuration" section at the bottom like below:



## Deleting installed Option Licenses:

### A) Via CLI interface

Uses “DCS\_” commands

DCS commands don't seem to be working correctly (in at least versions 5.9.1 and 5.9.4)

Note (8 March 2022): per JIRA ticket SSS-1254, DCS commands such as DCS\_GetOptions 0 aren't working

- **DCS\_GetOptions 0** lists the installed licenses (example below)

```
spadmin@Spectracom ~ $ DCS_GetOptions 0
DCS Get Options (4) available Licenses :
License 0: MULTIGNSS
License 1: AGPS Server
License 2: TIMEKEEPER
License 3: BroadShield
spadmin@Spectracom ~ $
```

- **DCS\_CheckOption**
- **DCS\_DeleteOption 0 #** deletes the options (where # is the Option Number desired to be removed)

**Caution:** Always verify the desired Options Number first, before deleting an Option, as the assigned Option number may be different in each unit (based on what other options were installed prior for installed)

**Example:** With TimeKeeper being Option 2, the command to remove it is **DCS\_DeleteOption 0 2**

### B) Another method to remove BroadShield software (not the license file remains installed)

- As BroadShield software is inherently removed during each software update, perform a standard update to newer version or a Force update to the same version currently installed. This will inherently remove broadshield

---

## 1223-SS00-0FS1: (“LAF GPI TimeStamper Option”) General Purpose Input Time Stamping

**Description:** License for GPI TimeStamper Option used with 1204-3C, RS422 4-IN, DB15 MALE option card.

- Software license associated with 1204-3C card
- refer to (In Arena): [https://app.bom.com/items/detail-spec?item\\_id=1230088220&version\\_id=10817184988](https://app.bom.com/items/detail-spec?item_id=1230088220&version_id=10817184988)

### minor software issue: general Purpose input timestamping Enable switch displayed in all browsers

Per Keith (4 May 2022): I noticed with at least version 5.9.4 (and v5.9.5 RC1) that the Enable switch for this function is present ([Management](#) -> [Network Setup](#) page), even though the applicable license and 1204-3C aren't installed. Checking with Eng to see if this is appropriate.

**Email from Gary Boff (4 May 2022):** Verified that this issue has been in the SW for quite a while. Looking at 5.8.2 the General Purpose Input Time Stamping” Service On/Off toggle switch is present. Enabling it has no effect other than making it look like its enabled.

---

## (Opt-IDM) (FKA “Opt-BSH) "SecureSync Interference Detection Suite Option” (fka BroadShield) Talen-x /embedded BroadShield interference and Spoofing detection software

- **Note:** Broadshield is enabled on our 10.15.108.11

### “LAF Broadshield Option” name change to “SecureSync Interference Detection Suite Option”

- Refer to ECO-2298 (Sept 2019)
- Change Option name from "LAF BroadShield Option" to "[SecureSync Interference Detection Suite Option](#)"

### Links/shortcuts

[Link to press release on a web page](#)

[Link to SecureSync with Broadshield information page](#)

**Link to BroadShield datasheet on our site:** [file:///C:/Users/Keith.Wing/Downloads/BroadShield\\_01-03-2020-1%20\(1\).pdf](file:///C:/Users/Keith.Wing/Downloads/BroadShield_01-03-2020-1%20(1).pdf)

**Link to SecureSync IDM suite on our site:** <https://www.rolia.com/solution/interference-detection-and-mitigation/>

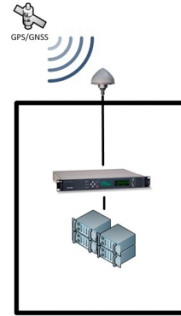
**Link to salesforce (pricing/ordering):** <https://na28.salesforce.com/01t1A0000056HWv?srPos=0&srKp=01t>

**Link to info about Opt-IDM in online SecureSync manual:**

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/Broadshield.htm?Highlight=bsh](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/Broadshield.htm?Highlight=bsh)

**Function:** BroadShield is an optional software module for SecureSync that is capable of detecting the presence of GPS jamming or spoofing in real time.

Detects Interference and Spoofing within the GPS signal and GPS spectrum  
 Over 75 jamming / spoofing detection algorithms  
 Works with our standard commercial GPS/GNSS receiver  
 Automatically enable/disable GPS during interference events  
 Status information through the UI  
 Integrated notifications and alarms



**Details:** Spectracom and [Talen-X](#) have aligned hardware and software development efforts to jointly develop, market and sell the most advanced PNT solutions, combining the strengths of leading **Spectracom Resilient PNT** products with Talen-X's **BroadShield** interference and spoofing detection suite.

The Spectracom SecureSync will take full advantage of BroadShield algorithms, which are known for meeting the requirements for Critical Infrastructure published by the US Department of Homeland Security (DHS). Beyond complying with DHS best practices, Talen-X has further enhanced the BroadShield algorithms to go beyond simply detecting various threats, also providing Spectracom SecureSync operators with detailed threat characteristics, real-time situational awareness and recorded data for post event forensic analysis.

---

### System requirements

- Strong GPS signal strengths
- **uBlox M8T GNSS receiver** (doesn't work with Trimble Res-T, or RES-SMT-GG receiver)
- Software **versions 5.7.1** or higher

---

### SecureSync Software changes associated w/BroadShield (descending order)/removal of Broadshield pseudod: new daemon created to pass ublox messages to the Broadshield option

### Removal of Broadshield and Timekeeper software from existing 5.8.4/5.8.5 (and future) SecureSync upgrade bundles (for both Options to be removed from units, when the bundles are obtained from us, after 10 Sept 2019)

- Refer to ECO-FAI-2269 (in Arena): [https://app.bom.com/changes/detail-summary?change\\_id=2397735912&](https://app.bom.com/changes/detail-summary?change_id=2397735912&)
  - Title of ECO: **"SecureSync 5.8.4 / 5.8.5 - Remove Timekeeper/Broadshield from software"**
  - **Effective date:** 10 Sept 2019
    - See additional info further below in **"Software updates remove BroadShield/Patch file"**

**Note:** If a new unit is inadvertently shipped without BroadShield installed/enabled (version 5.8.4 and above), see Ryan Johnson. I believe he can send a patch file which installs the software, so that it doesn't need to be returned to us, for it to be added in.

9:59 AM



[9:44 AM] Ryan Johnson

| SecureSync Version | BroadShield Version | Includes JADE |
|--------------------|---------------------|---------------|
| 5.9.x              | 5.7.6               | YES           |
| 5.8.x              | 5.2.2               | NO            |

(1 liked)

### Software Changes associated with Broadshield (in ascending order)

#### Version 5.9.0

- Per the Version 5.9.0 release notes: “Updated Broadshield support to version 5.7.6”

**Important Note from Ryan Johnson (19 April 2021)** You are correct - BroadShield 5.7.6 is only for SecureSync 5.9.X. Earlier versions of SecureSync (versions 5.8.9 and below) need BroadShield 5.2.2

#### Version 5.8.5 (July 2019)

- per the Version 5.8.5 release notes: “Updated Broadshield support to version 5.2.2”

#### Version 5.8.3 (Jan 2019)

- per the Version 5.8.3 release notes: “Updated Broadshield to version 5.1.1”

#### Version 5.7.1

- Introduce Talen-X BroadShield feature (requires purchasing license OPT-BSH)

#### Version 5.7.0

- [Jira ticket SSS-228] - BroadShield KTS Integration
- [JIRA ticket SSS-192] - BroadShield: Web UI control needed and Major Minor Alarms need to be disabled on startup
- [SSS-192] - BroadShield: Web UI control needed and Major Minor Alarms need to be disabled on startup

### Indications that Opt-BSH (or opt-Jade) is installed

- Unlike Opt-JADE, Opt-BSH requires a license file be installed (Opt-BSH license)
1. Like Opt-Jade, “**Monitoring**” button at top of browser will be present (with the License file installed, whether or not the BroadShield file has been installed yet/is installed)



2. Once the Opt-BSH license file has been installed (even if the BSH software file hasn't been installed yet) the CLI commands of **licenses** and **manifest** report BroadShield is installed (**options** command doesn't report BroadShield installed)

```
spadmin@Spectracom ~ $ licenses
0:BSH
spadmin@Spectracom ~ $
```

```
spadmin@Spectracom ~ $ manifest
#####
Thu Nov 11 16:07:13 UTC 2021
#####
SecureSync
Model No: 1200-003
Serial No: 17962
Power: AC 110/220
OSC : TCXO
GPS : SPS GNSS Rcvr
TEMP : EXT-TEMP
-----
Software      5.9.1
Timing System 3.5.9
Build Time    Nov 21 2020 03:45:29
-----
Linux Kernel: 4.14.34-gentoo-x64
-----
ETX Board: SOM-4466
-----
XO Oscillator Type: TCXO (1ppm)
-----
GNSS Receiver GPS 0 Mfr/Mdl: u-blox M8T
Versions: 3.01 1.10 22.00 00080000
-----
Option Card Slot 1: Empty

Option Card Slot 2: 1204-06
|->Card ID: 0x06
|->Card Version: 0x02
|->FPGA ID: 0x00
|->FPGA Version: 0x0000

Option Card Slot 3: Empty

Option Card Slot 4: Empty

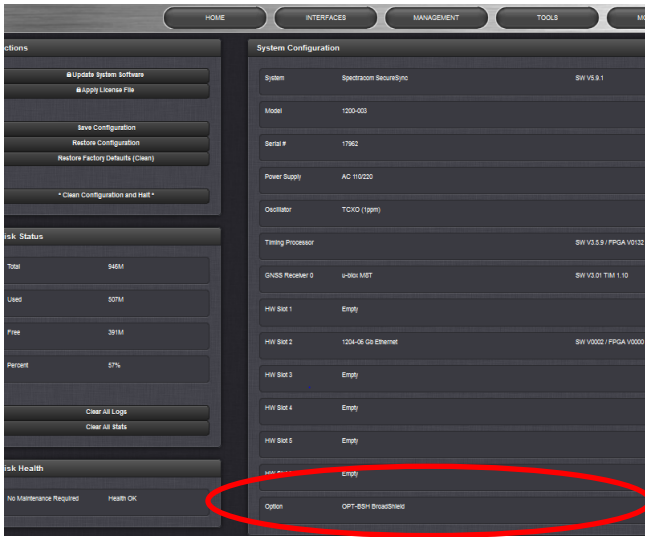
Option Card Slot 5: Empty

Option Card Slot 6: Empty
-----
DCS Get Options (1) available Licenses :
License 0: BroadShield
-----
Runtime: 0 days 0 hours 15 minutes (15 ticks)
spadmin@Spectracom ~ $
```

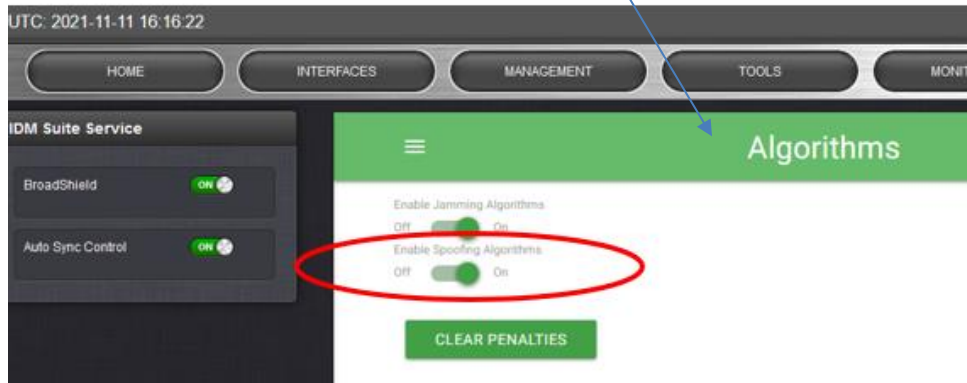
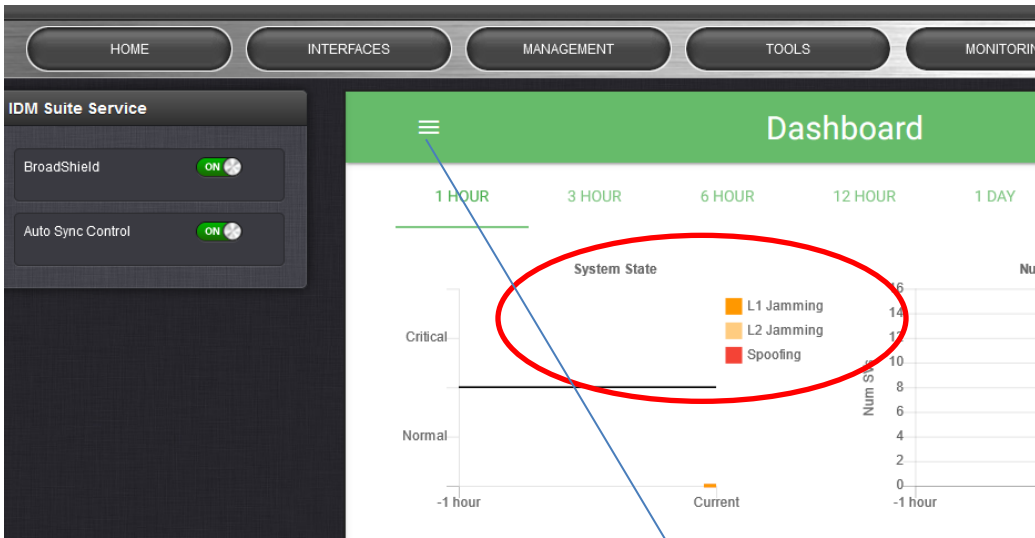
```
spadmin@Spectracom ~ $ options
1:None      4:None
2:Gb Eth    5:None
3:None      6:None
spadmin@Spectracom ~ $ licenses
0:BSH
```

- 3. Once the Opt-BSH license file has been installed (even if the BSH software file hasn't been installed yet) the bottom of the [Tools-> Upgrade/Backup](#) page and the Manifest log indicate BSH is installed.





**Verifying Opt-BSH license file is working (Spoofing is Enabled)**



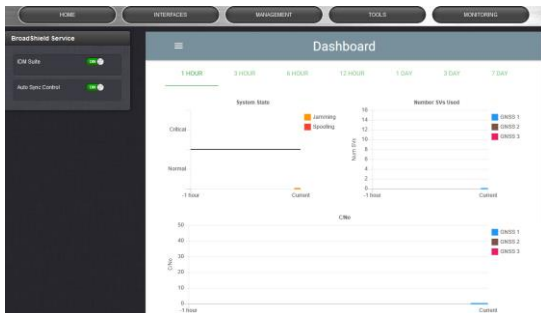
Software updates remove BroadShield/Patch files (“1200-SU02-B522.tar.gz” for 5.8.9 and below, or “1200-SU02-B76.tar.gz” for 5.9.0 and above) needs to be re-applied after each update

Symptoms of a software update being performed/patch needing to be applied ([Monitoring](#) -> [BroadShield](#) page)



Turning on IDM suite indicates BroadShield is enabled. But refreshing the page turns it back off again. HotPatch is applied similar to standard software update (only takes a couple minutes. Will report it failed. No reboot required)

(After patch has been applied):



**Link to BroadShield files to reinstall the software after software updates/replacing CF Card:**

- Refer to the following folder for BroadShield files and distribution instructions : [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Options\Opt IDM \(Broadshield\)\need to install hotpatch after software updates](#)

### Important Note about BroadShield software versions

- BroadShield **version 5.7.6** is **ONLY** compatible with SecureSync/NetClock software versions **5.9.0 and above**
- SecureSync/NetClock software **versions 5.8.9 and below** require earlier Broadshield **version 5.2.2** be installed
  - Installing BroadShield **5.7.6** on software **versions 5.8.9** and below will cause the BroadShield Option to keep turning off.

**Report of BroadShield file version currently installed**

**Monitoring -> Broadshied.**

Click  (to the left of “dashboard”)

Click “About”

Version

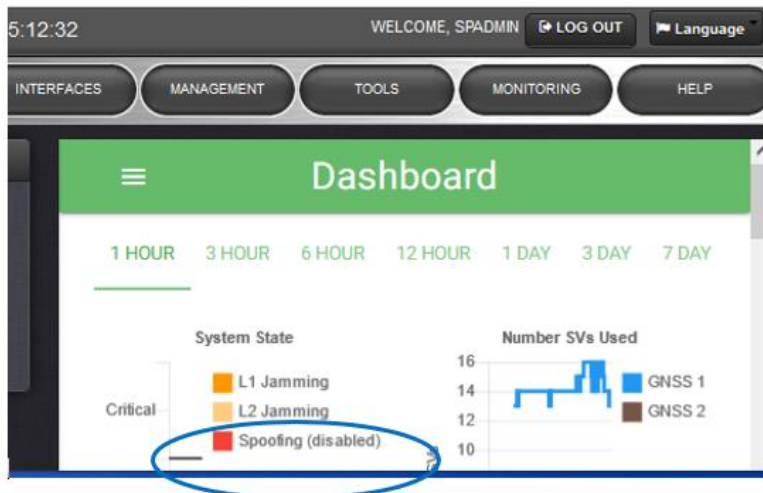
v5.2.2

Build Date

2019-03-04T20:44:09

## Deleting/removing either BroadShield software and/or Opti-Jade

- Refer to “Deleting installed Option Licenses” further above
- Note the BroadShield software can be removed. But Option JADE (Jamming, but no Spoofing detection) will remain enabled.



- The license file for Broadshield will remain (the Monitoring tab, with BroadShield in the drop-down, will still be visible. Clicking on BroadShield will show that BroadShield is not installed and can't be enabled)

## broadsheed.ini file/Configuration of BroadShield

- Refer to online SecureSync manual:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/Broadshield.htm?Highlight=broadshield](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/Broadshield.htm?Highlight=broadshield)

## broadsheed.ini file

path to the broadsheed.ini file: [home/spectracom/config/Talen-X/BroadShield.ini](http://home/spectracom/config/Talen-X/BroadShield.ini)

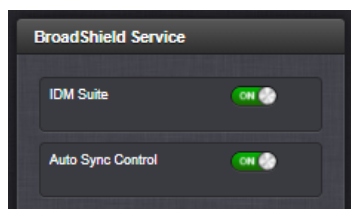
## “Talen-X/BroadShield.ini: Permission denied”

- refer to Salesforce case 172828

**Default state after installing license:** Broadshield is disabled after adding license file

## BroadShield Operation

### “BroadShield Service”



**IDM suite:** Turns IDM (BroadShield) either On or Off

**“Auto Sync Control”:** Two available Modes of operation for BroadShield (desire for Broadshield to not effect operation)

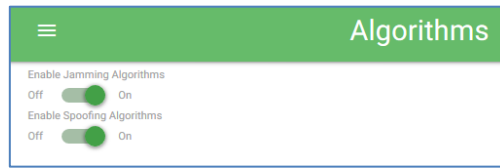
- The Broadshield service can be run in two operating modes:

- **BroadShield only:** In the event jamming or spoofing is detected, SecureSync will emit a Major Alarm, however it will continue to consider the GNSS reference as valid, i.e. it **will NOT go out of sync**.
- **Auto Sync Control:** In the event jamming or spoofing is detected, SecureSync will emit a Major Alarm **AND it will go into Holdover mode**.

## A) To configure the mode of operation

1. Navigate to **MONITORING > BroadShield**.
2. In the BroadShield Service panel on the left, configure the desired setting:
 

**Note:** Turning IDM Suite OFF and Auto Sync Control ON is an invalid setting and will cause a "Failed to connect to the unit..." error.
3. In the BroadShield Web UI on the right, navigate to **SETTINGS > ALGORITHMS**, and ensure that Jamming and/or Spoofing detection are enabled.



Main page below, with BSH v5.7.6 installed (and with "SETTINGS" on the left expanded down to see all selections)



## B) Dashboard



**Note:** A SecureSync reboot will reset all history data (it can still be retrieved via LOGS.)

### Dashboard

The dashboard panel displays up to 7 days of history data, and a real-time amplitude frequency spectrum. The headline background color indicates the current jamming/spoofing status: **red**= jamming or spoofing detected; **green** = no alarms at this time

### Top graph

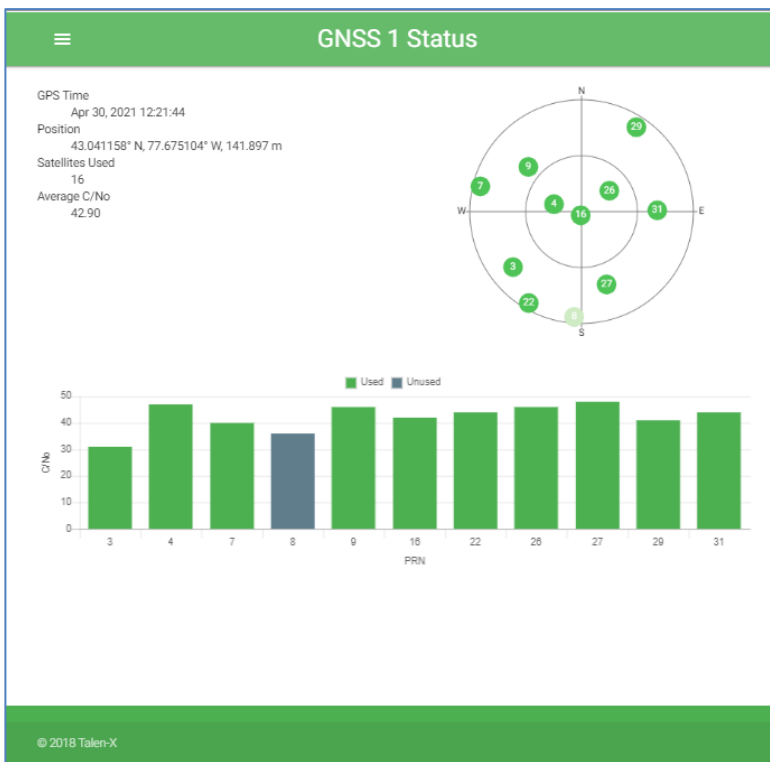
The Dashboard top graph displays the past signal level over time, divided into a Normal and a Critical signal level (separated by a red line). A blue line in the Critical zone indicates a potential jamming incident, while a green line indicates that SecureSync may be subject to a spoofing attack.

You can change the time scale by clicking on any of the labels between [1 HOUR](#) and [7 DAY](#).

### Bottom graph

The bottom graph labeled Spectrum visualizes the current signal over the GPS frequency band. Unusual amplitude spikes indicate a potential threat. If your system is equipped with more than one GNSS receivers, a green and an orange graph will indicate the signal level for additional receivers.

### C) GNSS 1 Status (Display only. No mouse-hovers)



#### Status information

- **GPS Time:** Time and Day as provided by SecureSync's GNSS receiver.
- **Position:** The position as determined by SecureSync's GNSS receiver.
- **Satellites Used:** The number of **GPS satellites** currently received by SecureSync. This number includes all satellites currently received for all enabled constellations (see [Selecting GNSS Constellations](#)). Note that BroadShield uses only GPS signals for jamming/spoofing detection.
- **Average C/No:** Average Signal to Noise (SNR) ratio. An average C/No value higher than 30 can be considered "good".

#### Skyplot graph

The center of the skyplot represents the antenna position. The skyplot shows all GPS satellites currently being tracked and – if enabled (under INTERFACES: REFERENCES > GNSS Reference: GNSS 0 > Edit button > Selected Constellations) – will also display all GLONASS satellites (numbered 65 and higher). Note, however, that GLONASS satellites will not be used by BroadShield. Galileo and Beidou satellites will not be displayed.

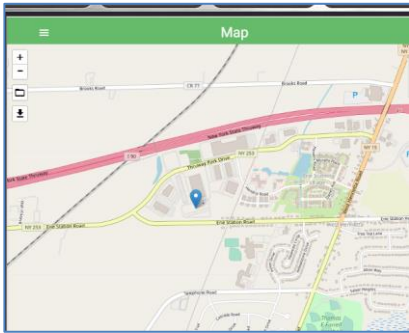
Note: Even though SecureSync may be configured to track multiple GNSS constellations (see [Selecting GNSS Constellations](#)), **BroadShield only uses GPS**.

#### Signal-to-noise bar graph

This graph visualizes the signal-to-noise ratio for up to 20 received satellites in real time. The satellites are numbered by their NMEA ID's (as in the skyplot mentioned above).

---

## D) Map (requires SecureSync to have Internet Access)

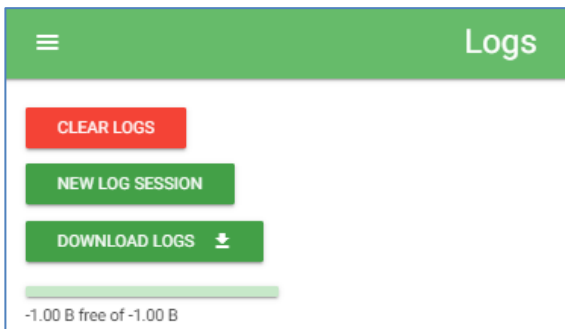


The map displays your current position, as reported by the GPS receiver. Should the displayed position differ from the actual antenna position, the GPS signal is likely spoofed.

Note that the map data is not part of the BroadShield software, but is downloaded from the Internet. Hence, this feature is only available if your SecureSync unit is connected to the Internet.

---

## E) Logs



- To **clear** all current logs stored on SecureSync, click CLEAR LOGS.
- To **start** a new log session, click NEW LOG SESSION.
- To **download** current logs, click DOWNLOAD LOGS.

**Note:** More details on logs further below

---



## F) SETTINGS sub-menus

### 1. RAPS

- Not sure what this is for
- Not observed in BSH software version 5.7.6 (was in earlier versions), must have been removed,
- IP address field at top can be edited

IP Addresses(Comma Seperated)  
e.g. 192.168.1.198,192.168.1.199,192.168.1.200

CANCEL SAVE ➤

### 2. BLISS

- Not sure what this is for
- First noticed in BroadShield version 5.7.6 (don't believe it was present in earlier versions)

Mode  
ALWAYS\_ON

Hardware Gain  
-20

Threshold  
900

ALWAYS\_ON  
ALWAYS\_OFF  
JS\_TRIGGERED

CANCEL SAVE ➤

### 3. Algorithms (“Enable Jamming Algorithms” / “Enable Spoofing Algorithms”)

Enable Jamming Algorithms  
OFF  ON

Enable Spoofing Algorithms  
OFF  ON

CLEAR PENALTIES

CANCEL SAVE ➤

This menu option allows you to disable/enable **Jamming** or **Spoofing**. Spoofing refers to impersonating the live-sky GNSS signal, thus "deceiving" the GNSS receiver, while Jamming refers to interference of the signal, i.e. making the live-sky GNSS signal unusable. Per default, both are Enabled.

### “Clear Penalties” button

- Not sure what this is for
- Doesn't appear to do anything when clicked

---

## 4. Remote API

- “Enable UDP snapshots” and “Enable Serial Snapshots” are both disabled by default
  - Both shown below as “Enabled”

Remote API

Snapshot Period (seconds)  
1

Snapshot Rx Id  
1

Enable UDP Snapshots  
Off  On

Hostname  
192.168.1.1

Port  
8777

Enable Serial Snapshots  
Off  On

Device  
ttyUSB0

Bauds  
115200

CANCEL SAVE

## 5. About

- Displays Version and Build Date of the BroadShield software.

About

Version  
v5.2.2

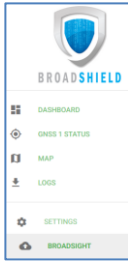
Build Date  
2019-03-04T20:44:09

---

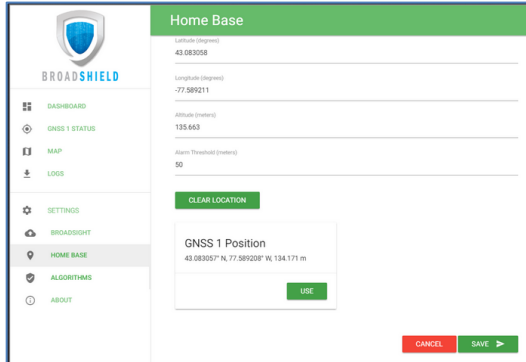
### Items which appear to have been removed in BroadShield v5.2.2

#### A) BroadSight (appears to have been removed in BroadShield v5.2.2)

- as of at least v5.9.0, Dec 2020, not supported for SecureSync



## B) “Home Base” position (optional) (Appears to have been removed in BroadShield v5.2.2)



- By setting the HOME BASE position you allow BroadShield to use this location as a reference position for spoofing detection:
  - Should BroadShield detect that the geographic position reported by SecureSync's GPS receiver seems to move beyond the set Alarm Threshold (even though SecureSync does not move), an alarm will be triggered.

### The standard use case is to make your GNSS 1 Position your HOME BASE:

1. Should the position fields be populated (other than the Alarm Threshold), click **CLEAR LOCATION** (this will prevent BroadShield from issuing an alarm once you SAVED the new position.)
2. Click **USE** in the GNSS 1 Position box to apply the settings.
3. The default Alarm Threshold is 50 m, i.e. any detected position shift beyond a 50-m circle around the HOME BASE position will cause an alarm. You can change this setting to adjust the sensitivity.
4. Click SAVE to accept the entered values.

A less common use case may be that you want to pre-set the unit's position for later use e.g., if the SecureSync unit will be deployed in a different location: Set a position manually by entering lat/long (format: xx.xxxxxx degrees) and alt. Note, however, that this may cause a spoofing alarm, since BroadShield detects a difference between the HOME BASE position and the GNSS position.

## Monitoring BroadShield / Associated Major alarm

- You can use the BroadShield Web UI to monitor the jamming/spoofing status, or the SecureSync Web UI. In the latter case, you will be informed of a Major Alarm.
- V5.9.4 update added one associated BroadShield trap and two associated SNMP Gets.

### If BroadShield detects a jamming or spoofing event, SecureSync will:

- emits a **“BroadShield Critical, Major Alarm”**
- SecureSync will go into Holdover (yellow HOLD status light) and – depending on the BroadShield Service setting and your SecureSync settings – will either remain in sync (green SYNC status light), i.e. it will continue to output time and frequency signals considered valid, or it will go out of sync (red SYNC light).



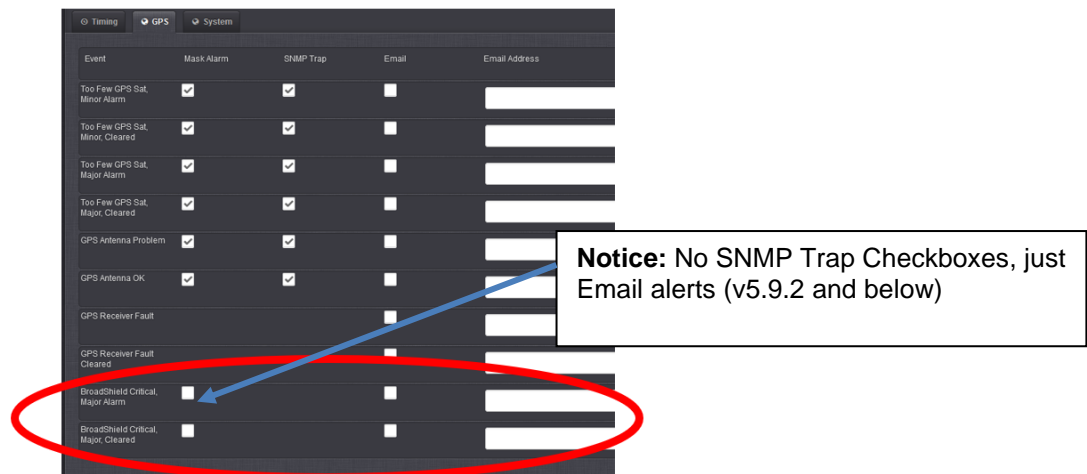
### Available Broadshield Notifications

- Only two notifications available for Broadshield (as of at least 5.8.9)

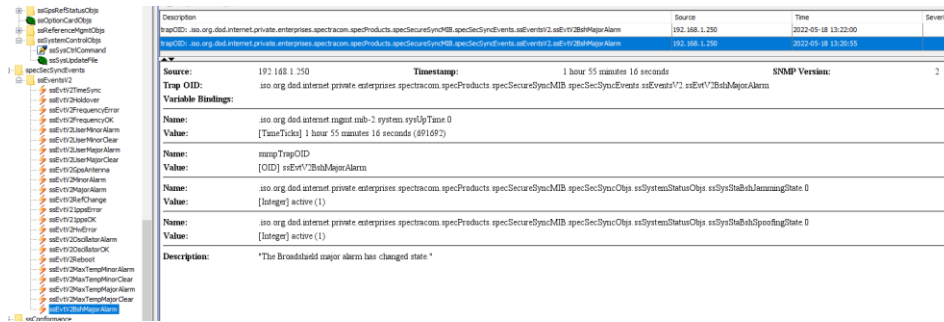
#### Email alerts/SNMP traps

- Version 5.9.3/5.9.4 (Nov 2021) added Broadshield SNMP trap enablement
- (Versions 5.9.2 and below) Email alerts only (no SNMP traps available)

- BroadShield alerts Enabled or masked in the **Management -> Notifications** page of the browser, **GPS** tab (only displayed if “IDM Suite” is enabled)



## A) SNMP Trap (1) for BroadShield (ssEventsV2.ssEvtV2BshMajorAlarm)



| Description                                                                                                                            | Source        | Time                | Severity |
|----------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------|----------|
| trapOID: iso.org.dod.internet.private.enterprises.spectracom.speProducts.speSecSyncMIB.speSecSyncEvents.sseEvtV2.sseEvtV2BshMajorAlarm | 192.168.1.250 | 2022-05-18 13:22:00 |          |
| trapOID: iso.org.dod.internet.private.enterprises.speProducts.speSecSyncMIB.speSecSyncEvents.sseEvtV2.sseEvtV2BshMajorAlarm            | 192.168.1.250 | 2022-05-18 13:26:55 |          |

| Source        | Timestamp                    | SNMP Version |
|---------------|------------------------------|--------------|
| 192.168.1.250 | 1 hour 55 minutes 16 seconds | 2            |

**Trap OID:** iso.org.dod.internet.private.enterprises.spectracom.speProducts.speSecSyncMIB.speSecSyncEvents.sseEvtV2.sseEvtV2BshMajorAlarm

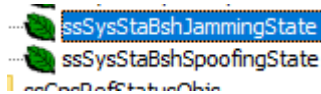
**Variable Bindings:**

|               |                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name:</b>  | iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0                                                                                     |
| <b>Value:</b> | [TimeTicks] 1 hour 55 minutes 16 seconds (491693)                                                                                      |
| <b>Name:</b>  | mempTrapOID                                                                                                                            |
| <b>Value:</b> | [OID] sseEvtV2.sseEvtV2BshMajorAlarm                                                                                                   |
| <b>Name:</b>  | iso.org.dod.internet.private.enterprises.spectracom.speProducts.speSecSyncMIB.speSecSyncObj.sSystemStatusObj.sSysStaBshJammingState.0  |
| <b>Value:</b> | [Integer] active (1)                                                                                                                   |
| <b>Name:</b>  | iso.org.dod.internet.private.enterprises.spectracom.speProducts.speSecSyncMIB.speSecSyncObj.sSystemStatusObj.sSysStaBshSpoofingState.0 |
| <b>Value:</b> | [Integer] active (1)                                                                                                                   |

**Description:** "The Broadshield major alarm has changed state."

- One trap is sent each time the BroadShield major alarm changes states (jamming /spoofing detected or no longer detected)
- The Trap varbinds indicate the current detection state of both Jamming and Spoofing (where “1” is actively being detected)

## B) SNMP Gets (2) for BroadShield (ssSysStaBshJammingState and ssSysStaBshSpoofingState)



### Issue: SNMP Gets for BroadShield not working in at least v5.9.4

- Refer to Salesforce Case **284662** / JIRA **SSS-1275**
- Two related SNMP Get objects were added in the MIB file, but not being found in the SecureSync software (SNMP No such object)

| Name/OID                   | Value /               | Type         |        |
|----------------------------|-----------------------|--------------|--------|
| ssSysStaBshJammingState.0  | (Snmp No Such Object) | NoSuchObject | 192.16 |
| ssSysStaBshSpoofingState.0 | (Snmp No Such Object) | NoSuchObject | 192.16 |

- Believe this was fixed in 5.9.5 update??

The following is an excerpt from internal Engineering notes about the v5.9.5 update:

**5.9.5 also contains fixes to address several issues (most customer reported, one internally identified):**

- Broadshield SNMP objects added but cannot be accessed via get or walk
- HSTS was added and can be enabled, but not working
- sendtrap help text updated to include Broadshield traps

## Real-time monitoring via web browser

- The BroadShield Web UI will also display real time signal status information, or a map status.

**Note:** If at any time you receive an error message “**Failed to connect to the unit**”, the SecureSync Web UI may have timed-out (see [Web UI Timeout](#)). Refresh your browser page to log back in.

## To open the BroadShield user interface:

Navigate to **MONITORING > BroadShield**. (If you cannot see the MONITORING button in the Primary Navigation Bar of the HOME screen, this license is not present.)

The embedded Broadshield Web UI will open, displaying the Dashboard and providing access to the following panels:

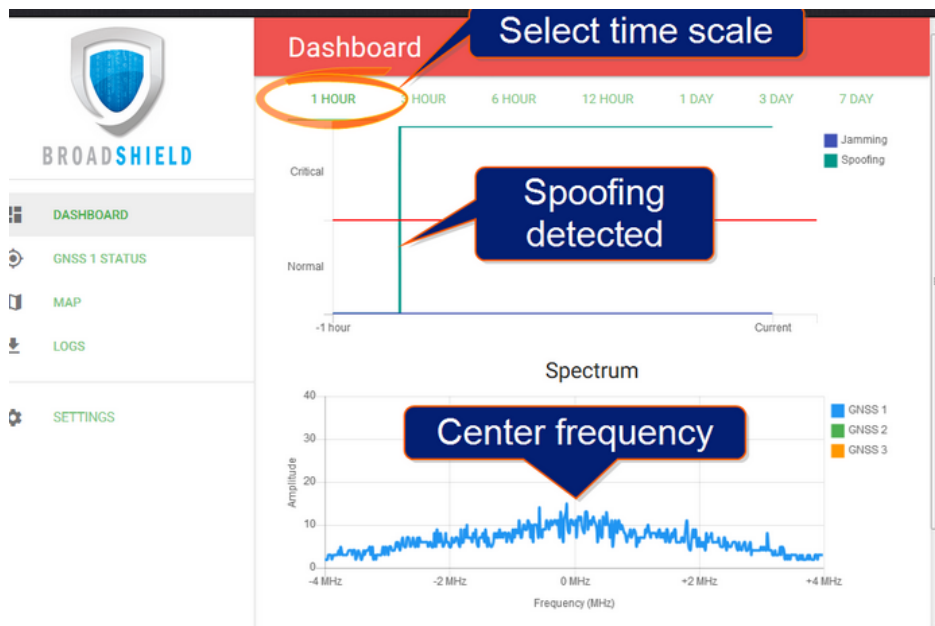
## DASHBOARD:

(*Monitoring* -> *BroadShield* page of the browser)

- The Dashboard panel displays up to 7 days of history data, and a real-time amplitude frequency spectrum. The headline background color indicates the current jamming/spoofing status:

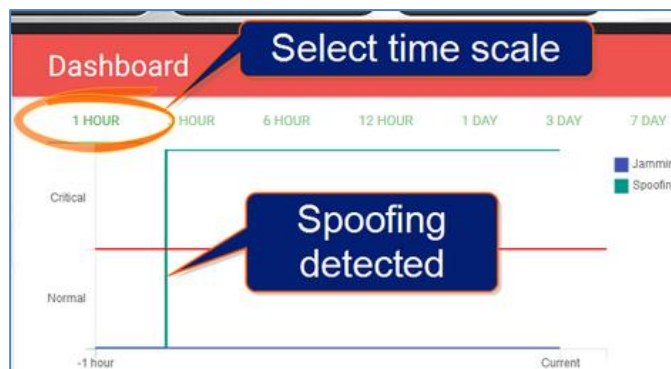
**red**= jamming or spoofing detected;

**green** = no alarms at this time



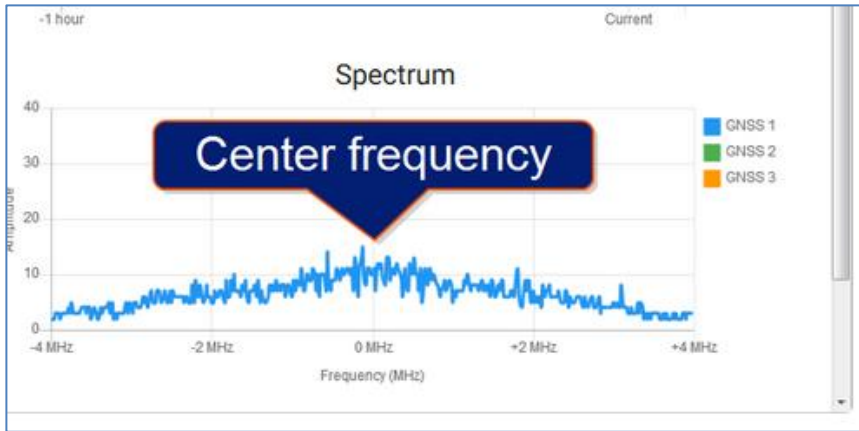
### A) Top graph of the dashboard (displays past signal level over time)

**Note:** You can **change the time scale** by clicking on any of the labels at the top (between “1 hour” and “7 days”)



- **Displays the past signal level over time**, divided into a Normal and a Critical signal level (separated by a red line).
  - A blue line in the Critical zone indicates a potential jamming incident, while
  - A green line indicates that SecureSync may be subject to a spoofing attack.
  - **Note:** A SecureSync reboot will reset all history data (it can still be retrieved via LOGS.)

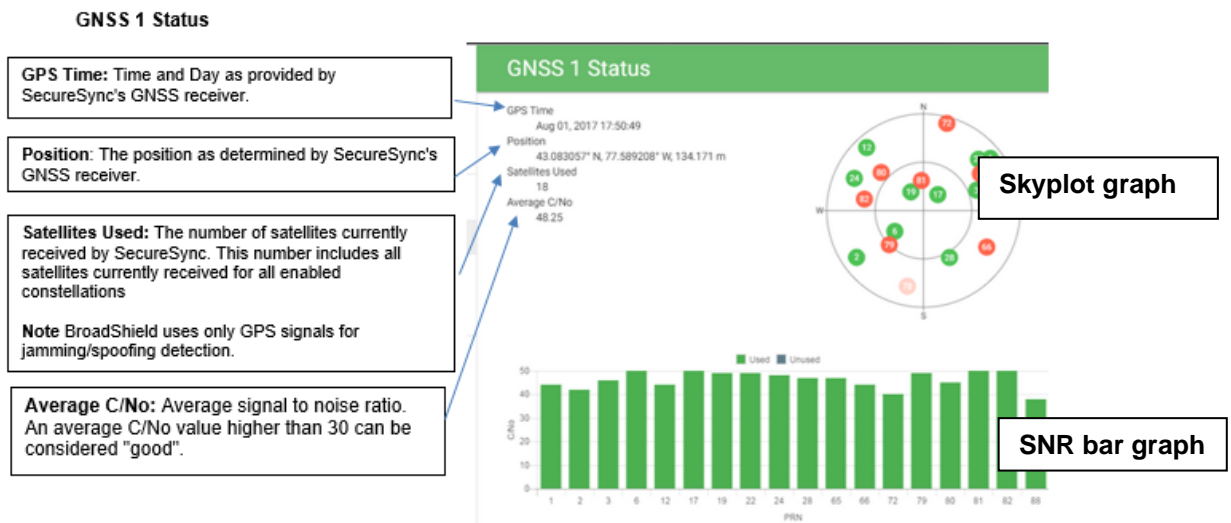
### B) Bottom graph of the dashboard (labeled “Spectrum”) (shows current signal over the GPS band)



- Visualizes the current signal over the GPS frequency band.
- Unusual amplitude spikes indicate a potential threat.
  - If your system is equipped with more than one GNSS receiver, a green and an orange graph will indicate the signal level for additional receivers.

### GNSS 1 Status (Skyplot graph)

- This graph visualizes the signal-to-noise ratio for up to 20 received satellites in real time. The satellites are numbered by their NMEA ID's (as in the skyplot mentioned above).



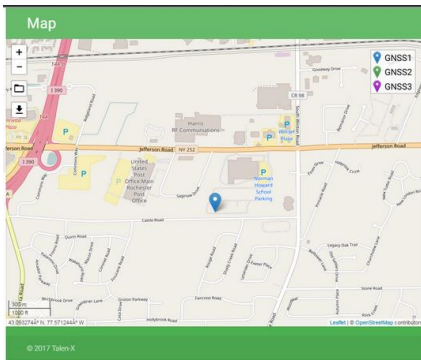
The center of the skyplot represents the antenna position. The skyplot shows all GPS satellites currently being tracked and – if enabled (under INTERFACES: REFERENCES > GNSS Reference: GNSS 0 > Edit button > Selected Constellations) – will also display all GLONASS satellites (numbered 65 and higher). Note, however, that GLONASS satellites will not be used by BroadShield. Galileo and Beidou satellites will not be displayed.

Even though SecureSync may be configured to track multiple GNSS constellations (see [Selecting GNSS Constellations](#)), BroadShield only uses GPS.

### “Signal-to-noise bar graph” (Below sky graph)

- This graph visualizes the signal-to-noise ratio for up to 20 received satellites in real time. The satellites are numbered by their NMEA ID's

## MAP (requires SecureSync to have Internet Access)



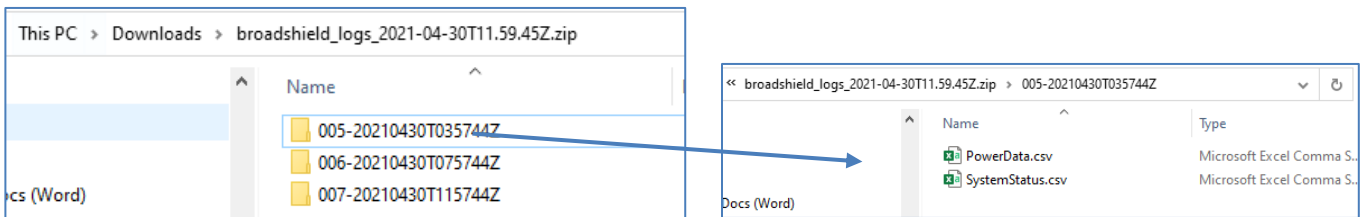
**Note:** the map data is not part of the BroadShield software, but is downloaded from the Internet. Hence, this feature is only available if your SecureSync unit is connected to the Internet.

- The map displays your current position, as reported by the GPS receiver.
  - Should the displayed position differ from the actual antenna position, the GPS signal is likely spoofed.

**BroadShield's dedicated Logs (SystemStatus.csv files) (note these are separate from the SecureSync's other available "System" logs)**

Available via "BroadShield browser pages and in Logs bundle

### Example of downloaded logs



Two csv log files in each folder

### A) PowerData.csv (no longer present in newer BSH version)

|   | A             | B          | C                        | D                 | E        | F        | G        | H        | I        | J        | K        | L        | M        | N        | O        | P        | Q        | R        | S   |            |  |
|---|---------------|------------|--------------------------|-------------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|-----|------------|--|
| 1 | FrameTime (s) | SystemTime | Power Detector L1 Center | Power Detector L1 | Power De | Power De | GNSS1 L1 | GNSS1 L1 | GNSS1 L2 | GNSS1 L2 | GNSS2 L1 | GNSS2 L1 | GNSS2 L2 | GNSS2 L2 | GNSS3 L1 | GNSS3 L1 | GNSS3 L2 | GNSS3 L2 | J/S | Confidence |  |
| 2 |               |            |                          |                   |          |          |          |          |          |          |          |          |          |          |          |          |          |          |     |            |  |
| 3 |               |            |                          |                   |          |          |          |          |          |          |          |          |          |          |          |          |          |          |     |            |  |
| 4 |               |            |                          |                   |          |          |          |          |          |          |          |          |          |          |          |          |          |          |     |            |  |

### B) JammingEvents.csv (present in newer BSH version)



|    | 1             | 2                    | 3    | 4           | 5           | 6           |
|----|---------------|----------------------|------|-------------|-------------|-------------|
| 1  | FrameTime (s) | SystemTime (UTC)     | Name | Description | Message     |             |
| 2  | 0.78          | 2022-03-04T11:26:26Z |      |             |             | 198         |
| 3  | 0.851         | 2022-03-04T11:26:26Z |      |             | I:185 Q:179 |             |
| 4  | 0.851         | 2022-03-04T11:26:26Z |      |             |             | 1135.603306 |
| 5  | 1.747         | 2022-03-04T11:26:27Z |      |             |             | 200         |
| 6  | 1.747         | 2022-03-04T11:26:27Z |      |             | I:184 Q:178 |             |
| 7  | 1.748         | 2022-03-04T11:26:27Z |      |             |             | 1281.02686  |
| 8  | 2.866         | 2022-03-04T11:26:28Z |      |             |             | 192         |
| 9  | 2.867         | 2022-03-04T11:26:28Z |      |             | I:186 Q:180 |             |
| 10 | 2.867         | 2022-03-04T11:26:28Z |      |             |             | 1822.107955 |
| 11 | 3.676         | 2022-03-04T11:26:29Z |      |             |             | 198         |
| 12 | 3.676         | 2022-03-04T11:26:29Z |      |             | I:186 Q:179 |             |
| 13 | 3.676         | 2022-03-04T11:26:29Z |      |             |             | 1714.582645 |
| 14 | 4.931         | 2022-03-04T11:26:30Z |      |             |             | 194         |
| 15 | 4.986         | 2022-03-04T11:26:30Z |      |             | I:185 Q:179 |             |
| 16 | 4.986         | 2022-03-04T11:26:30Z |      |             |             | 1714.582645 |

### C) SystemStatus.csv

|   | A             | B                   | C            | D              | E               | F                | G           | H           | I           |
|---|---------------|---------------------|--------------|----------------|-----------------|------------------|-------------|-------------|-------------|
| 1 | FrameTime (s) | SystemTime (UTC)    | System State | System Penalty | Jamming Penalty | Spoofing Penalty | GNSS1 State | GNSS2 State | GNSS3 State |
| 2 | 0.003         | 2021-04-30T03:57:44 | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 3 | 0.997         | 2021-04-30T03:57:45 | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 4 | 1.997         | 2021-04-30T03:57:46 | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 5 | 2.998         | 2021-04-30T03:57:47 | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 6 | 3.998         | 2021-04-30T03:57:48 | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 7 | 4.998         | 2021-04-30T03:57:49 | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 8 | 5.998         | 2021-04-30T03:57:50 | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |

Home -> Spectracom -> Log -> broadshield directory

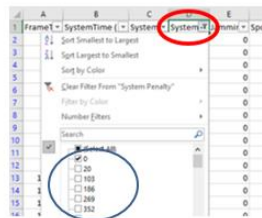


| Name                 | Date modified |
|----------------------|---------------|
| 001-20171005T152033Z | 10/5/2017     |
| 002-20171005T152625Z | 10/5/2017     |
| 003-20171005T192624Z | 10/5/2017     |
| 004-20171005T232623Z | 10/5/2017     |
| 005-20171006T032621Z | 10/5/2017     |
| 006-20171006T072620Z | 10/6/2017     |
| 007-20171006T112618Z | 10/6/2017     |
| 008-20171006T152617Z | 10/6/2017     |

Example SystemStatus.csv file:

| FrameTime (s) | SystemTime (UTC)     | System State | System Penalty | Jamming Penalty | Spoofing Penalty | GNSS1 State | GNSS2 State | GNSS3 State |
|---------------|----------------------|--------------|----------------|-----------------|------------------|-------------|-------------|-------------|
| 0.148         | 2017-10-09T11:25:54Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 0.997         | 2017-10-09T11:25:55Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 1.996         | 2017-10-09T11:25:56Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 2.997         | 2017-10-09T11:25:57Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 3.997         | 2017-10-09T11:25:58Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 4.997         | 2017-10-09T11:25:59Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 5.997         | 2017-10-09T11:26:00Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 6.996         | 2017-10-09T11:26:01Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 7.996         | 2017-10-09T11:26:02Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 8.996         | 2017-10-09T11:26:03Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 9.996         | 2017-10-09T11:26:04Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |
| 11            | 2017-10-09T11:26:05Z | NORMAL       | 0              | 0               | 0                | NORMAL      | DISABLED    | DISABLED    |

**Note:** In lieu of scrolling through the list to find if there are entries not containing “0s”, right click on a value in the **System Penalty** column, select “filter” -> “filter by selected cells Value”. Then left-click on the filter icon to the right of the System Penalty field. If values other than “0” are displayed, there are one or more fields that aren’t a “0 in this file



Fields in each csv file:

- FrameTime
- SystemTime (UTC)
- System State

**System Penalty: count of either jamming and/or Spoofing penalties**

**Jamming Penalty: count of jamming penalties**

**Spoofing Penalty count of Spoofing penalties**

**GNSS1 State: (“Home Base” position)**

**GNSS2 State (not currently used)**

**GNSS3 State (not currently used)**

**Note:** Having System Penalty (Jamming and/or spoofing penalties) numbers other than “0” doesn’t necessarily mean a problem should have been detected – the numbers have to actually exceed some unknown threshold to be considered a penalty and to assert associated alarms.

**Example entries of “System Penalty” fields not containing 0’s**

| FrameTime | SystemTime (UTC)     | System | System Penalty | Jamming Penalty | Spoofing Penalty | GNSS1 State |
|-----------|----------------------|--------|----------------|-----------------|------------------|-------------|
| 10316     | 2017-10-08T06:18:00Z | NORMAL | 999            | 999             | 0                | NORMAL      |
| 10329.998 | 2017-10-08T06:18:14Z | NORMAL | 999            | 999             | 0                | NORMAL      |
| 10338.999 | 2017-10-08T06:18:23Z | NORMAL | 999            | 999             | 0                | NORMAL      |
| 10339.998 | 2017-10-08T06:18:24Z | NORMAL | 999            | 999             | 0                | NORMAL      |
| 10340.999 | 2017-10-08T06:18:25Z | NORMAL | 999            | 999             | 0                | NORMAL      |
| 10346.998 | 2017-10-08T06:18:31Z | NORMAL | 999            | 999             | 0                | NORMAL      |
| 10364.998 | 2017-10-08T06:18:49Z | NORMAL | 999            | 999             | 0                | NORMAL      |
| 10405.998 | 2017-10-08T06:19:30Z | NORMAL | 990            | 990             | 0                | NORMAL      |
| 10485.998 | 2017-10-08T06:20:50Z | NORMAL | 692            | 692             | 0                | NORMAL      |
| 13020.059 | 2017-10-08T07:03:04Z | NORMAL | 1182           | 0               | 1182             | NORMAL      |
| 13021.061 | 2017-10-08T07:03:05Z | NORMAL | 1099           | 0               | 1099             | NORMAL      |
| 13022.179 | 2017-10-08T07:03:06Z | NORMAL | 1016           | 0               | 1016             | NORMAL      |
| 13023.066 | 2017-10-08T07:03:07Z | NORMAL | 933            | 0               | 933              | NORMAL      |
| 13024.058 | 2017-10-08T07:03:08Z | NORMAL | 850            | 0               | 850              | NORMAL      |
| 13025.058 | 2017-10-08T07:03:09Z | NORMAL | 767            | 0               | 767              | NORMAL      |
| 13025.998 | 2017-10-08T07:03:10Z | NORMAL | 684            | 0               | 684              | NORMAL      |
| 13027.06  | 2017-10-08T07:03:11Z | NORMAL | 601            | 0               | 601              | NORMAL      |
| 13028.183 | 2017-10-08T07:03:12Z | NORMAL | 518            | 0               | 518              | NORMAL      |
| 13029.063 | 2017-10-08T07:03:13Z | NORMAL | 435            | 0               | 435              | NORMAL      |
| 13030.06  | 2017-10-08T07:03:14Z | NORMAL | 352            | 0               | 352              | NORMAL      |
| 13031.066 | 2017-10-08T07:03:15Z | NORMAL | 269            | 0               | 269              | NORMAL      |
| 13032.062 | 2017-10-08T07:03:16Z | NORMAL | 186            | 0               | 186              | NORMAL      |
| 13033.062 | 2017-10-08T07:03:17Z | NORMAL | 103            | 0               | 103              | NORMAL      |
| 13033.998 | 2017-10-08T07:03:18Z | NORMAL | 20             | 0               | 20               | NORMAL      |

Jamming Penalties

Spoofing Penalties

**Rotation of Broadshield’s log (SystemStatus.csv files)**

➤ Per Paul M (9 Oct 17) If CF card usage is greater than 70%, Broadshield logs are deleted.

**Email from Paul Myers (10 Oct 2017)** I wanted to describe how BroadShield uses space on the disk for customer service knowledge.

This can be added to the manual, or other BroadShield documentation as Hendrik sees fit and used by customer service to support the product, however, it is intended to keep the system using no more than 70% disk space to support updates. Manual deletion of logs and A-GNSS files is supported in case needed and the updates in the future delete BroadShield logs and A-GNSS data because space is needed to perform the update. They are NOT preserved across updates.

Please read this email in its entirety and then feel free to re-organize/re-phrase the information or ask questions.

1. The BroadShield License OPT-BSH can be see using the license command line command, or by using the manifest command line or in the /home/Spectracom/config/manifest.conf or /home/Spectracom/log/manifest.log files.
2. When installed and enabled BroadShield will create logs in /home/Spectracom/log/broadshield in numbered folders.
3. To ensure the BroadShield logs do not use too much disk space, the older ones are deleted if the total disk space used in the SecureSync exceeds 70%. This can be if BroadShield logs use too much space or if other users of disk space increase their consumption. This can occur if a user loads an update or if other logs grow in size.
4. For example, the A-GNSS server feature creates Almanac and RINEX3 files in the /pub path, these files do not use a large amount of space unless multiple constellations are enabled and the number of days saved is large. Normally less than 30 days is used however, as many as 400 days can be saved. BroadShield logs will be

deleted if the overall system space needs increase.

- Note A-GNSS Server still cannot use GLONASS, without crashing for a u-blox M8T receiver, but Broadshield though it monitors GPS only can run with GLONASS enabled.
- Note to clear the all logs including the broadshield run “clearlogs” from the command line or clear them from the web ui.

To remove all A-GNSS server data, run clearagnss from the command line.

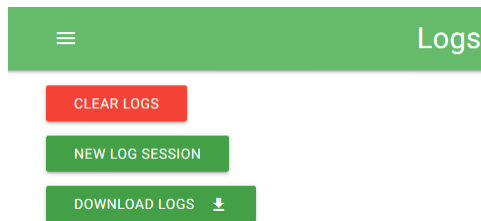
Note the installed software versions and licenses can be seen in the manifest.

ON an additional debugging note:

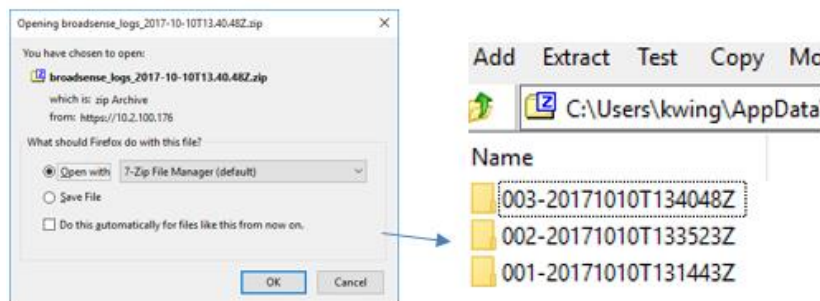
In 5.7.1 we added the manifest command and files as well as a runtime command line command.

To see how long the System and run ever use the “runtime” command, to see how long the linux system has been running since the last boot use the “uptime” command. Using these commands and the /home/Spectracom/log/manifest.log file entries you can see how long the system was running since the last boot and between reboots in the past.

### Clear/download logs (SystemStatus.csv files)



- To clear all current logs (SystemStatus.csv files) stored on SecureSync, click CLEAR LOGS.
- To start a new log session, click NEW LOG SESSION.
- To download current logs, click DOWNLOAD LOGS.



### Other “Spectracom” log fields which may also contain Broadshield entries

**Note:** Broadshield entries are inherently asserted/cleared each time the Broadshield option is enabled.

```
Oct 5 15:20:33 ohcntp2 ohcntp2: [system] BroadShield Critical, Major, Cleared
Oct 5 15:20:35 ohcntp2 ohcntp2: [system] BroadShield Warning, Minor, Cleared
Oct 5 15:20:35 ohcntp2 ohcntp2: [system] BroadShield Critical, Major, Cleared
```

#### A) Alarms.log

- Example entry Oct 8 02:41:02 ohcntp2 ohcntp2: [system] BroadShield Critical, Major Alarm

#### B) Events.log

➤ Example entries

```
Oct 5 15:20:33 ohcnpzp2 ohcnpzp2: [system] BroadShield Critical, Major, Cleared
Oct 5 15:20:35 ohcnpzp2 ohcnpzp2: [system] BroadShield Warning, Minor, Cleared
Oct 5 15:20:35 ohcnpzp2 ohcnpzp2: [system] BroadShield Critical, Major, Cleared
Oct 5 15:26:25 ohcnpzp2 ohcnpzp2: [system] BroadShield Critical, Major, Cleared
Oct 8 02:41:02 ohcnpzp2 ohcnpzp2: [system] BroadShield Critical, Major Alarm
Oct 8 02:41:02 ohcnpzp2 ohcnpzp2: [system] In Holdover
Oct 8 02:41:02 ohcnpzp2 ohcnpzp2: [system] 2017 281 02:41:02 000 SS: Reference changed to Time Ref: none PPS Ref: none
Oct 8 02:41:03 ohcnpzp2 ohcnpzp2: [system] Reference Change
Oct 8 02:41:04 ohcnpzp2 ohcnpzp2: [system] Reference Change (Cleared)
Oct 8 02:42:05 ohcnpzp2 ohcnpzp2: [system] BroadShield Critical, Major, Cleared
Oct 8 02:42:06 ohcnpzp2 ohcnpzp2: [system] Reference Change
Oct 8 02:42:06 ohcnpzp2 ohcnpzp2: [system] 2017 281 02:42:06 000 SS: Reference changed to Time Ref: gps0 PPS Ref: gps0
Oct 8 02:42:07 ohcnpzp2 ohcnpzp2: [system] No Longer In Holdover
Oct 8 02:42:08 ohcnpzp2 ohcnpzp2: [system] Reference Change (Cleared)
```

---

**Specific example of the benefits of having Broadshield available**

- both sets of logs below were from same customer/same site in Ohio (next to a trucking facility, often observing intermittent jamming). The first set (twice in the same day) shows the Rb oscillator going in and out of free-run until the jamming goes away. The second set shows the rb staying on free run until jamming stops.

**A) Broadshield option not available (two separate jamming events on the same day caused the Rb oscillator to go in and out of lock)**

```
Oct 5 07:00:46 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:00:46 000 XO: Ref Changed: old=gps0 new=none
Oct 5 07:00:46 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:00:46 000 XO: Phase Reference Invalid.
Oct 5 07:00:48 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:00:47 000 XOS: Rb track off -- free run
Oct 5 07:00:54 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:00:54 000 XO: Ref Changed: old=none new=gps0
Oct 5 07:00:54 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:00:54 000 XO: Phase Reference Valid.
Oct 5 07:02:28 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:02:28 000 XOS: Rb synchronized
Oct 5 07:03:00 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:03:00 000 XOS: Frequency error recalculated: -00.000023 (-2.337x10^-12)
Oct 5 07:31:31 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:31:31 000 XO: Ref Changed: old=gps0 new=none
Oct 5 07:31:31 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:31:31 000 XO: Phase Reference Invalid.
Oct 5 07:31:32 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:31:32 000 XOS: Rb track off -- free run
Oct 5 07:31:39 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:31:39 000 XO: Ref Changed: old=none new=gps0
Oct 5 07:31:39 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:31:39 000 XO: Phase Reference Valid.
Oct 5 07:33:14 ohcnpzp2 ohcnpzp2: [system] 2017 278 07:33:13 000 XOS: Rb synchronized

Oct 5 10:21:08 ohcnpzp2 ohcnpzp2: [system] 2017 278 10:21:07 000 XOS: Frequency error recalculated: -00.000011 (-1.192x10^-12)
Oct 5 11:02:10 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:02:10 000 XO: Ref Changed: old=gps0 new=none
Oct 5 11:02:10 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:02:10 000 XO: Phase Reference Invalid.
Oct 5 11:02:12 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:02:11 000 XOS: Rb track off -- free run
Oct 5 11:02:15 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:02:15 000 XO: Ref Changed: old=none new=gps0
Oct 5 11:02:15 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:02:15 000 XO: Phase Reference Valid.
Oct 5 11:03:49 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:03:49 000 XOS: Rb synchronized
Oct 5 11:04:05 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:04:04 000 XOS: Frequency error recalculated: 00.000059 (5.980x10^-12)
Oct 5 11:23:09 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:09 000 XO: Ref Changed: old=gps0 new=none
Oct 5 11:23:09 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:09 000 XO: Phase Reference Invalid.
Oct 5 11:23:11 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:10 000 XOS: Rb track off -- free run
Oct 5 11:23:13 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:13 000 XO: Ref Changed: old=none new=gps0
Oct 5 11:23:13 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:13 000 XO: Phase Reference Valid.
Oct 5 11:23:15 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:15 000 XO: Ref Changed: old=gps0 new=none
Oct 5 11:23:15 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:15 000 XO: Phase Reference Invalid.
Oct 5 11:23:17 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:17 000 XO: Ref Changed: old=none new=gps0
Oct 5 11:23:17 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:23:17 000 XO: Phase Reference Valid.
Oct 5 11:24:52 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:24:51 000 XOS: Rb synchronized
Oct 5 11:25:25 ohcnpzp2 ohcnpzp2: [system] 2017 278 11:25:24 000 XOS: Frequency error recalculated: -00.000024 (-2.483x10^-12)
```

Oct 5 12:01:16 ohcntp2 ohcntp2: [system] 2017 278 12:01:16 000 XO: Ref Changed: old=gps0 new=none

## **B) Broadshield available and active (oscillator remains in Holdover until Penalty event has cleared)**

Event started

Oct 8 00:47:10 ohcntp2 ohcntp2: [system] 2017 281 00:47:09 000 XOS: Frequency error recalculated: -00.000006 (-6.704x10<sup>-13</sup>)

Oct 8 02:41:03 ohcntp2 ohcntp2: [system] 2017 281 02:41:03 000 XO: Ref Changed: old=gps0 new=none

Oct 8 02:41:03 ohcntp2 ohcntp2: [system] 2017 281 02:41:03 000 XO: Phase Reference Invalid.

Oct 8 02:41:04 ohcntp2 ohcntp2: [system] 2017 281 02:41:04 000 XOS: Rb track off -- free run

Event ended

Oct 8 02:42:07 ohcntp2 ohcntp2: [system] 2017 281 02:42:07 000 XO: Ref Changed: old=none new=gps0

Oct 8 02:42:08 ohcntp2 ohcntp2: [system] 2017 281 02:42:07 000 XO: Phase Reference Valid.

Oct 8 02:43:42 ohcntp2 ohcntp2: [system] 2017 281 02:43:41 000 XOS: Rb synchronized

Oct 8 02:43:49 ohcntp2 ohcntp2: [system] 2017 281 02:43:48 000 XOS: Frequency error recalculated: -00.000002 (-2.917x10<sup>-13</sup>)

Oct 8 05:50:56 ohcntp2 ohcntp2: [system] 2017 281 05:50:55 000 XOS: Frequency error recalculated: 00.000005 (5.366x10<sup>-13</sup>)

## \*\*SS-OPT-JADE (SecureSync Jamming detection)

- Refer to ECO-2668 (in Arena at: [https://app.bom.com/changes/detail-summary?change\\_id=2403399054&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/changes/detail-summary?change_id=2403399054&orb_msg_single_search_p=1))
- In Salesforce: <https://orolia.lightning.force.com/lightning/r/Product2/01t0h000005onS9AAI/view>
- BroadShield software, minus “spoofing detection capabilities”

**P/N:** SS-OPT-JADE

**Function:** SecureSync Jamming detection (not spoofing detection, which is provided by Opt-IDM software). Per Salesforce “This software-only option for SecureSync adds GPS/GNSS signal jamming detection algorithm support”

Adds SecureSync Jamming Detection Suite support to SecureSync **with u-blox M8T GPS/GNSS** receiver (Note: Not available with SAASM GPS configuration, or with Trimble receivers (such as Res-SMT-GG and Res-T receivers)

### Associated software versions:

- **Main software versions:** v5.9.0 and above (~Jan 2021)
- **BroadShield version:** v5.7.6 and above

[9:44 AM] Ryan Johnson

| SecureSync Version | BroadShield Version | Includes JADE |
|--------------------|---------------------|---------------|
| 5.9.x              | 5.7.6               | YES           |
| 5.8.x              | 5.2.2               | NO            |

### EULA documentation/requirements

Requires customer to submit EULA document (as of at least the beginning of 5.9.0 being available)

**Part of:** Opt-IDM (BroadShield). Requires file **1200-SU02-B576** (SW FW, SYSTEM UPGRADE BROADSHIELD 5.7.6) or higher??

- **NOTE:** the license requires the IDM binaries to be installed via a patch. The master version of the patch is housed in **U:\Documentation\Released\Firmware\_Software**

Per Scott Zmuda (8 Nov 2021), the EULA is the same whether its for JADE or Opt-BSH (“The EULA is basically the same. No difference”)

### Enabling Opt-Jade vs Enabling Opt-BSH

Opt-Jade uses the same BroadShield install file as Opt-BSH (its not a dedicated file just for Jade). It’s whether or not the Opt-BSH license file (the other necessary file) is installed, which dictates whether Opt-Jade or Opt-BSH (Opt-IDM) will be active.

**Per Ryan Johson (8 Nov 2021)**

In terms of JADE vs. BroadShield implementation, think of it this way...

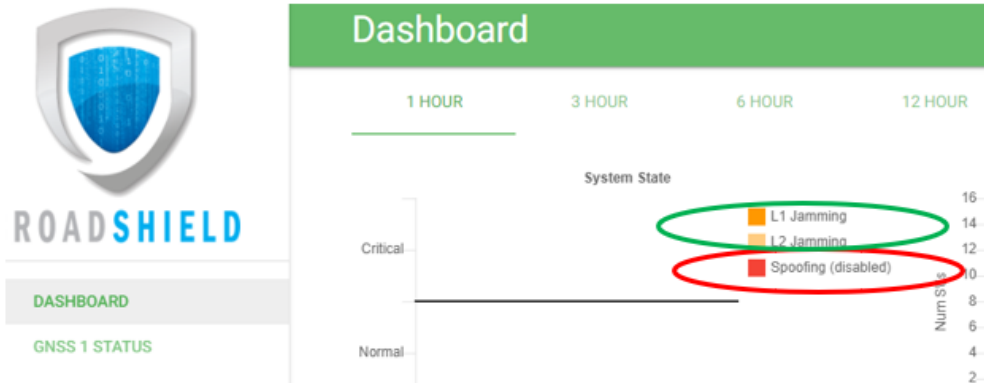
**Broadshield patch + OPT\_BSH license** = Full Broadshield w/ Jamming & Spoofing detection

**Broadshield patch (no license)** = “JADE” Broadshield w/ only Jamming detection

Basically the Broadshield application was modified such that the spoofing detection algorithms would only run in the OPT-BSH license was installed. The Jamming algorithms have nothing blocking them so they are always active.

## Indications that Opt-Jade (or opt-BSH) is installed

Per Keith (Nov 2021) the only report I could find to differentiate Opt-Jade (not Opt-BSH) being installed is in the Opt-BSH software itself:



As of at least versions 5.9.1 and below, it appears that the only indication that Opt-Jade (or Opt-BSH) is installed, is via the **Monitoring** button at the top of the browser page



- The CLI commands of **options** and **licenses** do not report Jade is BroadShield or Jade is installed.

```
spadmin@Spectracom ~ $ options
1:IRIG 2324:PTP
2:Gb Eth 5:ATC 232
3:485 RLY6:IRIG
spadmin@Spectracom ~ $ licenses
No licenses
```

- The **Tools-> Upgrade/Backup** page and the **Manifest** log do not indicate jade or BSH is installed.

## Opt-Jade Operation

Besides Opt-Jade not supporting Spoofing, there are NO other difference between the two. Refer to the Opt-BSH section (before OPT-Jade) for info on logs/operation of Jade/BSH.



---

## **\*\*SS-OPT-SKY (Opt-SKY/Skylight): Skylight option (indoor GPS system)**

**Note:** skylight antenna was discontinued August 2021

**Discontinued** (no last time buy) effective 27 Aug 2021

---

### **EOL PRODUCTS**

- Skylight antenna : EoL effective immediately, no LTB

- Can be applied in field via purchased license file
- Purchase of option includes specialized indoor antenna and SS OPT-GNS GLONASS option
- Skylight SecureSync is configured with a LPN OCXO oscillator (such as 1200-x2x)

**Our P/N:** SS OPT-SKY

#### **Links:**

- Link to Skylight datasheet (in Sharepoint): <https://oroliagroup.sharepoint.com/sites/oroliasalesmarketing/>
  - On our website: <http://spectracom.com/sites/default/files/document-files/skylight.pdf>
- Link to Skylight QuickStart guide (1200-5000-S051) in Arena: [https://app.bom.com/items/detail-spec?item\\_id=1202845058&version\\_id=10212762618&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=6410168528](https://app.bom.com/items/detail-spec?item_id=1202845058&version_id=10212762618&orb_msg_single_search_p=1&redirect_seqno=6410168528)
  - **Rev B (or higher) of this quickstart guide is for Skylight Phase 2:**
    - Note:** Skylight license enables Glonass and purchase includes the Skylight antenna.
  - **Rev A of this quickstart guide is for Skylight Phase 1 only (version 4.7L software)**
- Link to Skylight design info: <S:\Engineering\Projects\Skylight>

---

#### **Design Phases of Skylight**

##### **A) Skylight Phase 1 (RES-SMT receiver/4/7L software):**

- First unit shipped: 2/2/2012

##### **B) Skylight Phase 2: (skylight license, standard Res-SMT-GG receiver)**

- First unit shipped (RES-SMT-GG receiver cut-in ~end of Mar/Apr 2014)
  - **Our P/N:** SS OPT-SKY
  - Refer to the "Skylight" data sheet: [I:\Marketing\ Product Data Sheets \(archive\)\Time & Frequency References](I:\Marketing\ Product Data Sheets (archive)\Time & Frequency References)
  - Can be applied in field via purchased license file
  - Purchase of option includes specialized indoor antenna and SS OPT-GNS GLONASS option
  - Skylight SecureSync is configured with a **LPN OCXO** oscillator (such as 1200-x2x)

## Limitations of skylight antenna (with Rb oscillator and cable lengths)

### A) Rubidium oscillator (don't use indoor antenna when a Rb osci is installed)

- Skylight antenna should not be used with a Rubidium oscillator installed (skylight phase 1 or phase 2)
- At least with skylight phase 1, there were issues initially with using the skylight antenna with a Rubidium oscillator (Rb likes a continuous good reference for its disciplining). ~~Denis Reilly said (Aug 2016) this may no longer be an issue due to software changes associated with the Rb oscillator. But we haven't likely performed any more recent skylight testing to confirm this.~~

**(Update Note, March 2017):** this is still the case with Skylight phase 2, also, At least with skylight phase 1 (and now also with phase 2), there were issues initially with using the skylight antenna with a Rubidium oscillator (Rb osc likes a continuous good reference for its disciplining. Phase 2 not having Rb was confirmed by both Dave S and Tom R.

### B) Cable lengths

- For details: Refer to [\\*\\*Skylight antenna](#) section (a little further down in this doc)

## Requirements - Per the Skylight data sheet:

- Skylight does not work everywhere.
- A signal to noise ratio above about 30 dBc/N<sub>0</sub> at the antenna panel is required. This can be pre-tested using a handheld GPS meter (mobile phone apps available) to ensure suitability.
- Subterranean and other radio-isolated locations will still need to be synchronized using other techniques (such as over a network via a PTP master-slave combination) versus by GPS directly. However, exterior walls or walls across from a window in above ground floors of a building are likely candidates for Skylight. Even urban canyon situations can be considered as neighboring buildings can often redirect signals to the antenna panel that contain useful timing information for the Skylight system.
- The signal does not have to be available 24/7. By using a precise stable oscillator and our proprietary disciplining algorithms, Skylight needs the GPS signal for only a few hours a day. Often the RF noise is reduced at night which can allow Skylight to maintain legally traceable time even if signal acquisition is subpar during the day.
- The SecureSync unit will be required to be within 25ft (max 100ft) of the exterior wall where the antenna will be mounted.

**Email from Hickey (9 Aug 16)** Our Skylight™ SecureSync Time and Frequency Synchronization System provides GPS synchronization using an indoor antenna, designed specifically for situations where a rooftop antenna is not practical. SecureSync is a NetClock design derivative for our DoD/aerospace programs markets, offering mil-spec hardened chassis, wide operating temperature specifications, etc. We use a high sensitivity receiver, coupled with a unique advanced antenna designed to maximize GPS reception indoors, employing a stylish design so it can be installed in the optimal location for indoor GPS reception, eg. an office or conference room on an upper floor of the building. There is a premium for the SecureSync with these new features of ~\$3000 over a standard NetClock/GPS time server/antenna system.

Skylight Indoor GPS Timing System requires the HP Low Phase Noise OXCO oscillator and the GPS+GLONASS receiver. Skylight does not work everywhere. A GPS signal above approximately 30dBc/N<sub>0</sub> at the antenna panel is required - this can be pre-tested using a handheld GPS meter (mobile phone apps available) to ensure suitability. Subterranean and other radio-isolated locations will still need to be synchronized using other techniques (such as over a network via a PTP master-slave combination) versus by GPS directly. However, exterior walls or walls across from a window in above ground floors of a building are likely candidates for Skylight. Even urban canyon situations can be considered as neighboring buildings can often redirect signals to the antenna panel that contain useful timing information for the Skylight system. The signal does not have to be available 24/7, as by using a precise stable oscillator and proprietary disciplining algorithms, Skylight needs the GPS signal for only a few hours a day. Often ambient RF noise is reduced at night, allowing Skylight to sync up and maintain legally traceable time even if signal acquisition is subpar during the day. The SecureSync unit will be required to be within 25ft (max 100ft) of the exterior wall where the antenna will be mounted.

---

### \*\*\*Desire to update Skylight Phase 1 (4.7L software) to Skylight phase 2 to allow updating to current (and future) versions of software

- Per conversation with Dave Sohn, 5 Jan 2014, Skylight customer can return it to us to replace RES-SMT RES-SMT-GG receiver, update software to the latest version and apply skylight license here at factory. We agreed non-warranty upgrade cost of \$200.00 plus shipping fees.
- Refer to the knowledge base article on this topic.
- Will allow customers to upgrade to current and future versions of software (refer to the latest Release Notes for details on all changes that have been incorporated since 4.7L was released)

#### Email from Keith to a customer (5 Jan 15)

Regarding the desire to update Skylight software to a version beyond the current version of 4.7L. Skylight SecureSyncs with version 4.7L software installed at the factory have a special Model GPS receiver installed that is not the same as non-Skylight SecureSyncs have installed. This special Model receiver was used in earlier Skylights for its increased sensitivity specs with weaker GPS signals. This Model GPS receiver is only compatible with changes that were specifically incorporated in the version 4.7L software. Updating the software beyond version 4.7L with this receiver installed breaks the communications between the SecureSync and this receiver. This is why the Skylight software can't be updated beyond version 4.7L.

We have since changed the GPS receiver Model that is being installed in newer SecureSyncs. This newer GNSS (GPS/Glonass capable) receiver has similar sensitivity specs as the receiver that was installed in earlier Skylight SecureSyncs. If the installed GPS receiver in a Skylight is upgraded at the factory to this newer Model GNSS receiver and a special license key is installed, the Skylight software is then applicable with/can be updated with all standard, future SecureSync updates that may be released (it is no longer limited to version 4.7L software).

The GNSS receiver upgrade needs to be performed at the factory. The cost to update the receiver, install the license file and update the SecureSync to the latest version of software is our minimum repair fee of \$200.00 USD plus shipping fees. If you would like to return it to us for the receiver upgrade, let me know and I will assign an RMA Number. In order to assign an RMA number, I just need to know the desired return ship to address, to whom it should be made attention to (if not yourself) and the bill to address (if not the same as the ship to address).

Q (from same customer above) If we decide against the receiver upgrade, what kind of risk does it pose, and/or how long could we go without the upgrade before Spectracom strongly advises we do it?

**A Keith's reply:** There really isn't any risk with the update. We've been shipping the newer GNSS receivers in all SecureSyncs that have GPS capability (the vast majority of all SecureSyncs) since April. Spectracom has no recommendations to update the receiver. The only requirement to upgrade it is if you wish to incorporate all of the many software changes that have implemented in software updates since version 4.7L was released. This includes both newer features (such as an improved web browser interface) as well as software enhancements.

The software version 5.1.7 Release Notes I previously emailed you can provide you with a list of changes that have been added since version 4.7L was released. There is one section for Features added and a second feature for software enhancements. If you would like to incorporate the changes, we can upgrade the receiver for you. But if you are happy with the software as it currently is, there is no need to replace the receiver. I don't suspect there will ever be any other reasons that the receiver will need to be upgraded, other than personal desires to have newer software- or if something was to happen to the receiver in the future requiring it to be replaced).

---

### Non-Low phase Noise OCXO oscillator installed (such as Rubidium Oscillator or standard OCXO)

**25 March 15 after talking with Dave Sohn (regarding Skylight Phase 2)** The data sheet specs using a SecureSync with a low phase noise OCXO installed (023). Based on anticipated periods of Holdover when using an indoor antenna, skylight is best tailored to using the characteristics of the LPN OCXO. The Rb oscillator having its own internal disciplining is not conducive to periods of expected Holdover, so it's best not to pair skylight with a Rb. Though we discipline the standard OCXO, it's not optimized for skylight. However, it can still be used with Skylight.

#### Rubidium oscillator with Skylight option

**Per Dave Sohn, 13 March 2014**, Skylight is not currently setup to work with a Rubidium SecureSync. Rubidium support for Skylight is not scheduled at this time.

We added support for 3.5 hour Rubidium SRO disciplining support in SecureSync several releases ago. If you believe that is enough for Skylight to operate then it is available already. If we want our own disciplining controlling the Rubidium, which will allow more flexible installation, then it is not and we haven't scheduled that. I have a prototype of that, but it isn't fully tested.

## \*\*Skylight antenna (1213-0000-0600)

**Discontinued** (no last time buy) effective 27 Aug 2021

### EOL PRODUCTS

- Skylight antenna : EoL effective immediately, no LTB



### Skylight Indoor GPS Timing System

Indoor Antenna Panel Solution for GPS Timing

GET A QUOTE

### Open a New Window to Accurate Time for Your Network.

Even though synchronizing network master clocks and time servers to GPS is well-known as the standard for the most time-sensitive applications, some data centers and critical server locations are not conducive to traditional roof-top GPS antenna installation. Skylight™ provides a solution. Consistent



### Links/Documentation for the skylight antenna

- **Link to Skylight data sheet:**
- **Link to Skylight QuickStart guide** (1200-5000-S051) in Arena: [https://app.bom.com/items/detail-spec?item\\_id=1202845058&version\\_id=10212762618&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=6410168528](https://app.bom.com/items/detail-spec?item_id=1202845058&version_id=10212762618&orb_msg_single_search_p=1&redirect_seqno=6410168528)
  - Note this document should have info on the antenna, but as of Rev B, it doesn't discuss the knob or jacks.
  - **Rev B (or higher) of this quickstart guide is for Skylight Phase 2:**
    - Note:** Skylight license enables Glonass and purchase includes the Skylight antenna.
  - **Rev A of this quickstart is for Skylight Phase 1 only (version 4.7L software)**
- Link to Process Detail (1213-0000=0600=PD) in Arena: [https://app.bom.com/items/detail-spec?item\\_id=1202837891&version\\_id=10228803578](https://app.bom.com/items/detail-spec?item_id=1202837891&version_id=10228803578)
- Antenna P/N (1213-0000-0600) in Arena: [https://app.bom.com/items/detail-spec?item\\_id=1202835940&version\\_id=10222045508](https://app.bom.com/items/detail-spec?item_id=1202835940&version_id=10222045508)

**Warranty period for Skylight antenna assembly:** Per Dave Sohn- 1 year warranty (not 5 year warranty)

### Skylight Antenna/Anc kit:

- **Our P/N: 1200-S001-0601** (in Arena): [https://app.bom.com/items/detail-spec?item\\_id=1202845074&version\\_id=10221321568&](https://app.bom.com/items/detail-spec?item_id=1202845074&version_id=10221321568&)

➤ **Anc kit consists of:**

- SecureSync (with Trimble Res-SMT receiver)
- Indoor GPS antenna
- 25 foot antenna cable (**CA01R-0NSA-4025** Cable Assembly, N-SMA, LL RG-58, 25 foot)

**Skylight antenna gain (actual antenna within the skylight housing)**



**Mobile GPS/GIONASS Antenna with LNA**

**Model: DS-28**

WI-RD-D-027 V1.0

Compact & Sensitive GPS/GIONASS antenna with ESD Circuit Protection for Mobile Applications



©2012 San Jose Technology, Inc.

➤ **MFG/Model:** Synergy Systems P/N [10501201G-1](#) Model DS-28

- **Our P/N:** E025R-0001-0009
- Refer to “WI-RD-D-027DS-28\_Catalog\_V1.0\_20121228” (in Arena):  
[https://files.bom.com/download/llbv8z2ufiqgeAIKpDc6cEVFIUNKQW0/hrwzqtmtctvefbjgcuzklwknbgldvnmqx/WI-RD-D-027DS-28\\_Catalog\\_V1.0\\_20121228.pdf](https://files.bom.com/download/llbv8z2ufiqgeAIKpDc6cEVFIUNKQW0/hrwzqtmtctvefbjgcuzklwknbgldvnmqx/WI-RD-D-027DS-28_Catalog_V1.0_20121228.pdf)

| SANAV                                                            |                                                                                                 |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>Applications:</b>                                             |                                                                                                 |
| • Automobile GPS/Glonass Receiver/Car Tracking Navigation System |                                                                                                 |
| • AVL / Fleet Management Systems                                 |                                                                                                 |
| • External Antenna for Handheld GPS/Glonass and Navigator        |                                                                                                 |
| <b>Specification:</b>                                            |                                                                                                 |
| <b>Physical Condition</b>                                        |                                                                                                 |
| Construction                                                     | Polycarbonate: radome at top, die-cast shell at bottom; rubber gasket for water seal in between |
| Dimension                                                        | 46.27mm (L) x 38.19mm (W) x 12.26mm (H)                                                         |
| Weight                                                           | 30 grams (excluding cable & connector)                                                          |
| Standard Mounting                                                | Magnet mount with two magnets & screw mount                                                     |
| Optional Mounting Plate                                          | Customized metal sheet                                                                          |
| <b>Cable &amp; Connector</b>                                     |                                                                                                 |
| RF Cable                                                         | 5 meter RG174/U (standard) cable, other length available                                        |
| Pulling Strength                                                 | 6 kg @ 5sec with molded plastics on connector end for strain relief                             |
| Connector Available                                              | BNC,TNC,PME (to be adapted), GTS, MCX (OSX), SMA, SMB or SMC in straight or right angle         |
| Optional Adapters                                                | Universal Connector Adapter (PME to TNC/BNC/SMA/SMB/MCX)                                        |
| <b>Antenna Element</b>                                           |                                                                                                 |
| Polarization                                                     | R.H.C.P. (Right Handed Circular Polarization)                                                   |
| Gain @ Zenith                                                    | 1.5 dBi typical                                                                                 |
| Axial Ratio                                                      | 90° : 3 :0dB max.                                                                               |
| Low Noise Amplifier                                              | Mounted on the 70mm x 70mm square ground plane                                                  |
| Gain                                                             | 27dB @ 3V                                                                                       |
| Bandwidth                                                        | 43 MHz min. @S11<-10 dB                                                                         |
| Noise Figure                                                     | 1.5dB Typical                                                                                   |
| Supply Voltages                                                  | 2.3 ~3V Dc                                                                                      |
| Current Consumption                                              | 3V : 10.6mA±1mA, 5V : 21mA ±1mA                                                                 |
| Output Impedance                                                 | 50 ohm                                                                                          |
| Output VSWR                                                      | 2.0 max.                                                                                        |
| <b>Overall Performance (Antenna Element, LNA &amp; Cable)</b>    |                                                                                                 |
| Center Frequency                                                 | 1575.42 MHz ± 10 MHz & 1602 MHz ± 8 MHz                                                         |
| Gain                                                             | At 90° 27 ± 3dB (cable loss) Note:1                                                             |
| Output Impedance                                                 | Mounted on the 70mm x 70mm square ground plane                                                  |
| VSWR                                                             | 50 ohm                                                                                          |
| Environmental Conditions                                         | 2.0 max.                                                                                        |
| Operation temperature                                            | -40°C to +55°C                                                                                  |
| Storage temperature                                              | -40°C to +55°C                                                                                  |
| Relative Humidity                                                | 95% non-condensing                                                                              |

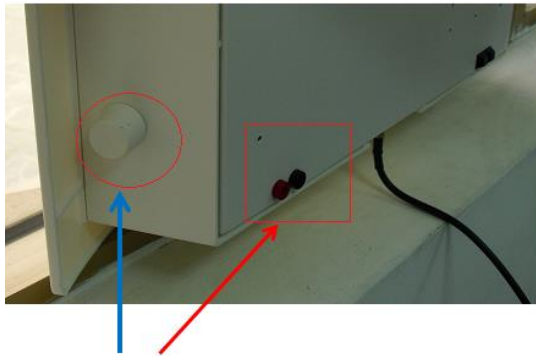
- **27 dB gain**

**Email from Eric Girard (14 Oct 2020)** I looked at the documentation in Arena. I found that the Skylight antenna is mounted with an GPS/GLONASS mini antenna -E025R-0001-0009 - from Synergy – Gain would be 27 dB @ 3V

---

**Skylight phase 1 and phase 2 antenna P/N: 1213-0000-0600**

- Rev A is the phase 1 antenna (GPS only)
- Rev B is the phase 2 antenna (GPS and Glonass)



**Knob and red/black jacks**

- **Knob:** The Skylight antenna has decorative LEDs built into the faceplate and the knob is a brightness control for the LEDs.
- **Jacks:** The red and black jacks are so you can swap the internals 180 degrees to have the antenna face inwards or outwards.

---

**\*\*Skylight Installation:**

- Refer to Skylight quickstart guide (1200-5000-S051) in Arena: [https://app.bom.com/items/detail-spec?item\\_id=1202845058&version\\_id=10212762618&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=6410168528](https://app.bom.com/items/detail-spec?item_id=1202845058&version_id=10212762618&orb_msg_single_search_p=1&redirect_seqno=6410168528)

**Length of antenna cable included with skylight antenna / desire to extend cable length**

- Skylight antenna includes 25 ft cable
- “The SecureSync unit will be required to be within 25ft (max 100ft) of the exterior wall where the antenna will be mounted”
- The additional cable length is highly recommended to be low loss. Such as LMR-400 or equivalent.

**Email from Rom Richardson (13 Mar 17)** The maximum cable length is determined by signal loss(attenuation) at 1.575 GHz in the cable.

Maximum cable loss (attenuation) should be 7 dB.

For example; typical RG316 cable has attenuation of 33 dB/100 feet at 1.5 GHz.

$33\text{dB}/100\text{ft} = .33/\text{foot}$

$7\text{dB}/.33\text{dB}/\text{ft} = 21\text{feet}$

This is a general rule and the reception might be much worse and Skylight might be unusable in a server room.

Skylight should not be used with Rubidium units.

**Email from Dave L (24 Jan 17)** The Skylight antenna option comes with a 25 foot cable as you know. It can be extended another 100 feet if necessary but the shorter the cable the better performance you will achieve.

If you do need to extend the cable, please use a low loss type cable such as our LMR 400 equivalent.

**Requirements - Per the Skylight data sheet:**

- Skylight does not work everywhere.
- A signal to noise ratio above about 30 dBc/N<sub>0</sub> at the antenna panel is required. This can be pre-tested using a handheld GPS meter (mobile phone apps available) to ensure suitability.

- Subterranean and other radio-isolated locations will still need to be synchronized using other techniques (such as over a network via a PTP master-slave combination) versus by GPS directly. However, exterior walls or walls across from a window in above ground floors of a building are likely candidates for Skylight. Even urban canyon situations can be considered as neighboring buildings can often redirect signals to the antenna panel that contain useful timing information for the Skylight system.
- The signal does not have to be available 24/7. By using a precise stable oscillator and our proprietary disciplining algorithms, Skylight needs the GPS signal for only a few hours a day. Often the RF noise is reduced at night which can allow Skylight to maintain legally traceable time even if signal acquisition is subpar during the day.
- The SecureSync unit will be required to be within 25ft (max 100ft) of the exterior wall where the antenna will be mounted.

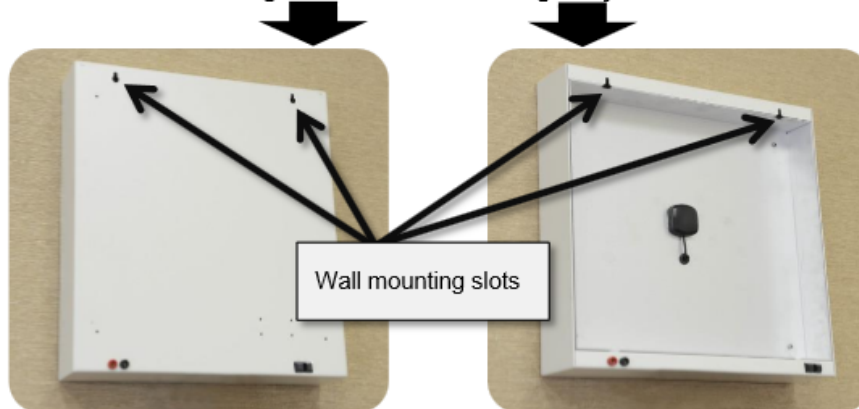
## Choose a Location for the Indoor Antenna

The location of the antenna strongly affects the performance of the system. Characteristics of an ideal location for placement are:

- High in the building to minimize obstructions from other buildings and natural features.
- Near windows or exterior walls facing the exterior of the building.
- An area with the number of walls between the antenna and the exterior of the building minimized.
- Certain window coatings dramatically attenuate GNSS signals, so an exterior wall may be a better location than facing a window.
- Away from areas with significant amounts of electronic equipment, such as a lab or server closet.
- Away from grids of metal, like a room of metal framed office cubes or lab benches, as this can reduce the available GNSS signals.

Although the characteristics described above are indicators of a good location, plan on experimenting to find the best location for the antenna, since it can be difficult to predict actual reception quality of different locations.

The antenna can be mounted **facing towards** or **facing away** from the wall:



Mounting the antenna facing towards an exterior wall often leads to the best reception.

Skylight customers need to enter their location to help the GPS get started. Starting on page 11 there is a nifty section about finding your location which could be cut and pasted to other customers who want to find their location.

## The key steps to getting it working are:

### Location/orientation

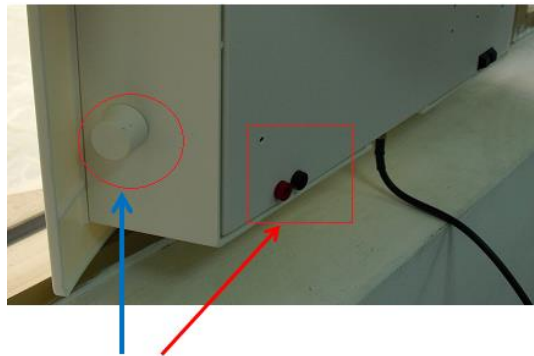
1) Think about where to put it. GPS isn't designed to work indoors, so the signals we are catching are very weak. It usually takes some experimentation

**Email from Mike Sander to Instinet (4/13/12)** To find a location for it where the signals are strong enough. Page 2 of the manual lists some considerations for good and bad locations.

- Set the UTC offset, instructions are on page 3, section 5.
- Set the location. See page 3, section 4. And the section starting on page 11.
- Follow the procedure on page 6, section 8 to evaluate positions.

**Try locating the antenna on an exterior wall away from any windows/try on an interior wall facing an exterior wall**

**Note: I believe the "option to reverse the antenna facing by switching the direction of the front plate" Dave mentions in his email below is referring to switching the red and black jacks on the back of the antenna:**



**Jacks:** The red and black jacks are so you can swap the internals 180 degrees to have the antenna face inwards or outwards.

**Email from Dave Sohn (17 Nov 16)** This is a skylight antenna, not the standard window mount. There is likely low-e coating in the windows, which is interfering with the reception. There are a couple things to note because of that, and that it is a skylight antenna. If he has a portion of exterior wall that is not metal/glass, he should try that. Also, the antenna is collecting energy through the front, so there is the option to reverse the antenna facing by switching the direction of the front plate. He might also try mounting on an opposite wall facing the outside.

### Installation concerns:

- SNRs really need to be in the 30s to achieve initial sync.

If the signal strength is reported in the low 20's, then it's not good enough to make the first fix.

**Email from Denis Reilly:** As a rule of thumb, we've found that it is difficult to get a Skylight to lock on any satellite signal if they are all below about 25 SNR.

### Emails from Mike Sander to improve Skylight reception

My biggest worry is that customers won't put any effort into finding a good location for the antenna. There are lots of pointers about good and bad locations in the manual. If they think about it and have even a basic understanding of what kinds of things block radio signals, (metal, electronics, or thick layers of concrete or stone) they should be okay.

In general, the signal is most affected by metal and electronics. So co-locations are tricky for indoor GPS.

Getting it above the ceiling tiles might help, but typically we don't see much signal coming in through the ceiling, even on a one story building. This is probably because of the grids of metal that are common in the roof construction. We focus on getting it near exterior walls or windows.

**Email from Denis Reilly**



Is the antenna mounted on anything metal? We have found that if the antenna chassis is in contact with metal – especially on a server rack – it can cause problems with reception.

### Questions to ask/things to look at:

1) Are they really not getting sync? You can get a cut-and-paste of the GPS Qualification log (Tools -> Logs page of browser) and see if the sync values are all zeros.

What kind of SNRs are they seeing?

- 0-20: noise
- 20-27, 28: weak signals, if it could acquire, it would probably continue to track
- 29 and up : I expect it to acquire

And what are the typical higher values of SNR are you seeing? (From that same table on the Status->Inputs->GPS page) As a general rule they need to get up to about 30 to acquire a satellite, and then it will track the satellite down to the low 20s.

- 1) Have they entered the location (what is the address)? Get a copy of the journal log to see if the location is correct
- 2) What's the address of the co-location site? I'll see what I can tell about the building construction and possible obstructions outside the building.
- 3) If they can open the window and the glass is the issue, they may be able to let it acquire satellites and download almanac data through an open window, kind of like a kick-start, and then see if it continues to sync through the walls or windows afterwards.
- 4) Confirm that the unpainted side of the antenna box, with the little black antenna unit, is facing towards the outside.
- 5) The further they can get the antenna unit from metal the better (such as metal filing cabinets and metal file racks that should be moved, if possible).
- 6) Small changes in antenna placement can make a big difference.
- 7) Small changes in the location can make a difference. For example, if you happen to have the antenna up against a metal stud in the wall, moving it 8 inches over might make all the difference. Use the procedure on page 6, section 8 to decide how long to try a particular location.
- 8) Have they entered the UTC offset?
- 9) How long have they run it at the location? We recommend about an hour, if they are seeing satellites. Then, if it doesn't sync, they should move it.
- 10) If they have low E glass windows (bad for RF signals), they should try moving the unit to an exterior wall.
- 11) How far is the antenna from an exterior wall? It's encouraging that you can put it against an exterior wall.
- 12) Is the antenna mounted on anything metal?
- 13) Note: We have found that if the antenna chassis is in contact with metal – especially on a server rack – it can cause problems with reception
- 14) What kind of a space do you have at the co-location? Is it a rack? Or a cage? Do you have space to get the antenna away, even a foot or two helps, from other electronics?
- 15) Are you seeing any satellites on table at the bottom of the Status->Inputs->GPS page?
- 16) An unlikely location for a successful installation would be deep in the interior of a co-location, with metal cages, metal racks and lots of servers between you and the exterior.
- 17) Is the antenna mounted on anything metal? We have found that if the antenna chassis is in contact with metal – especially on a server rack – it can cause problems with reception

### **There are several things we can try:**

- 1) I'd like to see another screen shot of the GPS status page. And please watch it for a few minutes to confirm that the SNRs, 30, 29, 28 that we were seeing yesterday are characteristic. Even if you were mostly seeing mid-20's SNR values, I would expect it to go into sync eventually. It's puzzling that you haven't gone into sync with the SNRs we saw yesterday.
- 2) If you send me a copy of the logs, I can look through them for unexpected entries.

### **Here is the procedure for exporting log files:**

- 1) On the Skylight web UI, Tools->Upgrade/Backup window, "Configuration" tab.
- 2) On the line, "Save Log Files", select "Enabled" and click "Submit"
- 3) This creates, on the SecureSync, the file /home/spectracom/xfer/log/SecureSync.log
- 4) Then you need to use ftp to connect to the SecureSync and get the file.
- 5) If you don't have a FTP utility on the laptop, you can use the windows command line FTP.
- 6) You can always try moving the antenna, and then leaving it at the new position for about 20 minutes. The best orientation for the antenna is point the side with the unpainted ground plane and the little black antenna module towards the outside. It sometimes helps if you send me a picture of the antenna location, I may see something that will help.

### **Email from Denis Reilly to a customer (5/10/12)**

I am the Project Manager for Spectracom's Skylight product. Wade let me know that you have set up the unit. Based on your description below, it looks like the unit is working fine, but I've included a few quick things for you to check when you get the time to.

It looks like you have found the page that lists the GPS Input Status ("On-Board Reference" on the Status > Inputs page). If that page shows that the "1PPS Validity" and "Time Validity" is OK, then your installation is working.

You can get information on the quality of your synchronization by going to the "Status > Time and Frequency Status" page. You should see the Synchronization state set to "OK", with the Time and 1PPS sources both set to "GPS 0". You can see how good the synchronization is under "Estimated Time Error".

Keep in mind that there will be some times where the Skylight unit can't get a good enough signal to maintain sync. At those times, you should see on the Time and Frequency page that the unit is in Holdover. During this period, the unit keeps time using its high-quality internal oscillator, and our Estimated Time Error is calculated using the characteristics of the oscillator.

I would be happy to take a look at the server if you would like me to. In particular, after the unit has been running for a while we can take a look at the system logs to find out when the unit may have gone out of sync, and the general signal quality we are getting over time. We can look at the logs directly on the unit, or I can tell you how to retrieve the logs via FTP so you can send them to us.

### **Email from Denis Reilly to Mauricio Terrats (5/25/12)**

We've discussed this within our Engineering team here, and we have determined that the antenna is probably too close to the server rack, and there is too much interference from the equipment. We strongly suggest that you move the antenna. We can offer a few suggestions:

- The cover is purely cosmetic. Although our tests indicate that the cover doesn't affect reception, you may wish to try it with the cover off if it is in a location where the appearance of the antenna doesn't matter.

- We have found that for customers that must locate their antenna near a server rack, the best place to locate it may be on the top of the rack, with the antenna facing up towards the ceiling. The cover can be put on the back of the unit: consider moving the cover to the back of the unit and resting the antenna on the cover in an attempt to shield the metal of the antenna box from the server rack.

I understand that this unit is installed at a remote location, but if it would be possible to try the antenna in a few different orientations it might be helpful. Even closing the door and placing the antenna on the other side of the door (so it is facing out while the door is closed) can be helpful. Facing the antenna away from any interference sources (even if it is facing into a wall) would be ideal.

---

## Troubleshooting /skylight issues (besides just signal strengths being too low)

GPS Receiver is reporting its tracking several satellites (more than 4), but the SecureSync is not going into Sync (even though the GPS survey is complete and everything else looks good). Also, the bottom of the Status -> Inputs, GPS page is showing all 0's for the ID fields and SNR fields. GPS is a "not valid" reference.

This can be a parsing issue due to Archive software version 4.7L being properly installed, but the wrong KTS version is installed. The KTS version (as reported in the Tools-> Versions page) should be at version 2.7L. If it's been updated beyond 2.7L, it needs to be downgraded to version 2.7L by Force updating the SecureSync using the 4.7L update file.

It will take a little time for the SecureSync to synchronize to GPS in a new location. I would give it a few hours. If not synced within that time here are few things to check:

- Are you really not getting sync? You can check the GPS Qual log and see if the sync values are all zeros or not.
- What kind of SNRs are you seeing in the Status/Inputs/On board reference – GPS :
- 0-20 – noise
- 20-27,28 – weak signals, if it could acquire, it would probably continue to track
- 28 and up – I expect it to acquire
- Have you tried manually entering the location?
- Have you entered the UTC offset?
- Try moving the unit to an exterior wall like you suggested where it is not looking through Low-E glass.
- Make sure the unpainted side of the antenna box, with the little black antenna unit, is facing towards the outside.
- The further you can get the antenna unit from metal the better. In the picture I see metal filing cabinets and a metal file rack that I would move if possible.
- If you can open the window, do this and let it acquire satellites and download almanacs through an open window, kind of like a kick-start, and then see if it continues to sync through the walls or windows afterwards. The GPS Receiver needs to get a initial fix on the location which typically takes about 45 minutes with good reception.

See if any of these suggestions work and let me know you progress. Again if you have any questions just let me know.

---

## Skylight SecureSync

### Skylight receiver

- Refer also to the receiver section of the customerserviceassistnace document

### Skylight phase 2 only

- Uses same RES-SMT-GG GNSS receiver that is used on other SecureSyncs shipped after ~ Mar/Apr 2014

### Skylight phase 1 only

- GPS receiver P/N: MP30R-0GPS-0006 (Trimble Naelcom Res-SMT GPS receiver)
- Link to Part Spec record: I:\Engineering\Engineering Shared\Spectracom Parts ROHS\MPxxR-xxxx-xxxx\MP30R-xxxx-xxxx

**Note:** GPS receiver must be version 1.01 firmware

---

### Skylight Serial Number (I believe this is for Skylight Phase 1 only)

As reported at the top of the **Tools -> Versions** page of the browser, Skylight SecureSyncs will have an "R" in their Serial Number (Representing a "retrofit" was performed).

### Res-SMT receiver installed indication (Skylight phase 1 only)

As reported at the top of the **Status -> Inputs, GPS** page of the browser, SecureSyncs with a RES-SMT receiver installed (instead of Res-T receiver) will indicate "Trimble Resolution SMT" (instead of "Resolution T").

### Compatibility of Skylight SecureSync with other GPS antennas (besides the specially designed indoor Skylight antenna we normally include)

**Email Keith sent to a customer, based on info from Denis Reilly (12/20/12)** The Skylight SecureSync is compatible with other "RF style" GPS antennas (those antennas that output/pass raw 1.5GHz GPS signal to the GPS receiver. Some GPS antennas output RS-485 data, as the receiver is in the antenna housing. The SecureSync is not compatible with this type of antenna). However, just keep in mind that the Skylight SecureSync includes a specially designed GPS antenna for the ability to be able to receive very weak GPS signals, while standard antennas are designed to receive much stronger signals that are located outdoors, with a good view of the sky.

---

### Archive and KTS Software Versions for Skylight Phase 1 SecureSyncs (as of 20 Dec 2012)

Software update when Skylight installed: The upgrade process is the same, but they can only upgrade to other Skylight versions.

Per Denis Reilly, there has been only one SecureSync software update associated with sklight units. This was version 4.7L, the first release to make Skylight available. No other subsequent updates have been released yet that can be applied to these units.

The Skylight SecureSyncs use a res-SMT receiver which uses different interface commands than the Res-T receiver uses. So applying a non-Skylight version will prevent the unit from being able to talk to the receiver.

**Important Note:** Currently, all Skylights MUST have Archive **version 4.7L** and **KTS version 2.7L** installed.

**PTP Option Card version:** According to Denis Reilly, B30 is compatible w/skylight

I believe the following Alarm log entry is an indication that a Skylight had been updated to a different version other than 4.7L, so it was no longer communicating with the GPS receiver:

Dec 19 22:00:02 Spectracom spectracom: [system] Failed to read Qualification Log from KTS (GPSD)

New page for Skylight installation (described further below) is not available in 4.7L. It MAY someday be added in a future release for Skylight, but is not available now!

### **If a skylight unit happens to be updated with a non-skylight software version (any version besides 4.7L is installed)**

- Have the customer send us a screenshot of the Tools -> Versions page of the browser to us. This will show the current software module versions and how many, if any, PTP Option cards are installed (which make fixing this issue much more difficult, due to early version update issues associated with the PTP cards).
  - Forward the screenshot to Denis Reilly and work with him for assistance with resolving this software incompatibility issue.
- 

## **Skylight Web browser/operation**

### **A-GPS/A-GNSS client/server (AGPS/Assisted GPS/ Assisted-GPS/Assisted GNSS)**

**Note:** For more information about A-GPS, refer to websites such as: [http://en.wikipedia.org/wiki/Assisted\\_GPS](http://en.wikipedia.org/wiki/Assisted_GPS).

#### **Two variants of A-GPS/A-GNSS**

##### **A) Server: A-GPS/A-GNSS rinex server (A-GPS server/A-GNSS server)**

- Allows a SecureSync to operate as a server, providing A-GPS ephemeris and almanac data to other devices e.g., a Spectracom GSG-series GNSS simulator. Requires purchase of A-GNSS license file (**SS-Opt-AGP**)
- refer to (Salesforce) <https://na28.salesforce.com/01tC0000004KRDS?srPos=0&srKp=01t> and (in this doc) [\\*\\*\(SS-OPT-AGP\) Rinex Server Option](#) for additional details.

##### **B) Client: (A-GPS client/A-GNSS client)**

- Used to send assistance data to the GPS receiver. This is most useful in areas with poor GPS reception.

#### **Software versions associated with A-GPS/A-GNSS**

##### **1. Update Version 5.8.0 (May 2018) Glonass support**

- Per 5.8.0 Release Notes: “A-GNSS Server RINEX3 and Almanac file creation now supports GLONASS”

##### **2. Update Version 5.2.1: Added Rinex server license/improved A-GPS**

- Added Assisted GPS Rinex server license, and improved A-GPS functionality

**Note:** Version 5.2.1 has an issue where ephemeris/almanac data is only sent for one satellite instead of all satellites. Being addressed with a patch.

##### **3. Update Version 5.1.3**

- A-GPS was added to all SecureSyncs/9400s in software version 5.1.3
- A-GPS is primarily for Skylight but is not limited to skylight.
- A-GPS is used to download ephemeris/almanac data from the Internet, to speed up time to first fix (TTF) and to help the receiver detect weaker signals that it may otherwise not be able to find.,
- Requires the network have a connection to the Internet to be able to work.
- CDDIS (Crustal Dynamics Data Information System)

## Rinex Server address

- In at least versions 5.1.3 and 5.1.4, Link to server is hard-coded in software: <ftp://cddis.gsfc.nasa.gov>  
**Customer email** - "I noticed that the SecureSync is periodically attempting a FTP (TCP protocol, port 21) connection with IP address 128.183.20.84 (reverse DNS lookup resolved to **cddis.gsfc.nasa.gov**)"

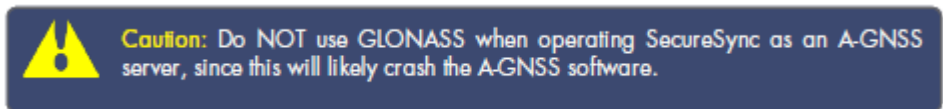
## Configuration of A-GPS

### Version 5.8.0 (May 2018) Glonass support

- Per 5.8.0 Release Notes: "A-GNSS Server RINEX3 and Almanac file creation now supports GLONASS"

**Note (versions 5.7.3 and below only):** GLONASS constellation being enabled (**Interfaces** -> **GNSS 0** page) will cause problems.

*From the user manual:*



**Email from Paul M (8 Nov 17)** Hmm... If I recall correctly GLONASS is not supported in A-GNSS Server RINEX generation for u-blox per release notes.

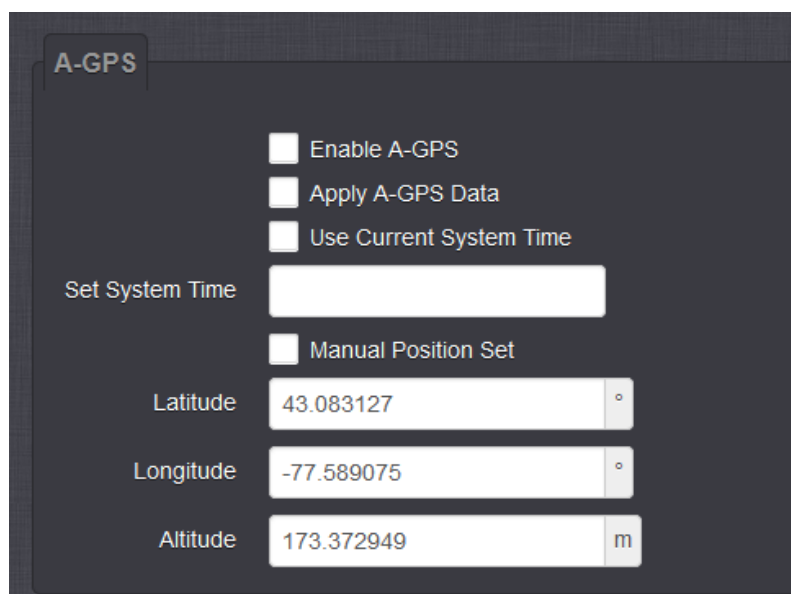
You need to know what constellations he is testing and I assume Mobile/Land configuration at least GPS only maybe GPS+GAL or GPS+GAL+BDS

I admit I do not recall testing in mobile mode, but I don't recall a reason it would not work. MAYBE I have forgotten a reason, but I can't recall one now...

You should have a unit in your test rack with u-blox M8T 3.01 TIM 1.10 and 5.7.1 which can be configured for testing.

I placed an engineering unit in test in GPS+GAL+BDS, turned on AGNSS server to collect data and placed it in mobile mode and will let it run with BroadShield with ALL licenses running.

A-GPS is configured in the **Interfaces** -> **GNSS Reference** page of the browser. Then click on the "Gear" box between "GNSS 0" and the indication of how many satellites are being tracked (below the photo)



**A-GPS**

- Enable A-GPS
- Apply A-GPS Data
- Use Current System Time

Set System Time

- Manual Position Set

Latitude

Longitude

Altitude  m

- A-GPS: – This feature is intended to be used to provide assistance data to the GNSS receiver. This is most  
pg. 230

commonly used in areas with poor GPS reception

- Enable A-GPS: This feature is used to turn on A-GPS functionality in the SecureSync. By enabling A-GPS the SecureSync will apply A-GPS data to the GNSS receiver automatically on startup if the GNSS reference is invalid.
- Apply A-GPS Data: When this option is selected SecureSync will immediately apply the time, position and satellite data to the receiver. Time and position are user configurable, the SecureSync collects A-GPS satellite data from an external source automatically.

### Version 5.8.0 (May 2018) Glonass support

- Per 5.8.0 Release Notes: "A-GNSS Server RINEX3 and Almanac file creation now supports GLONASS"  
**CAUTION:** Any parameters entered under "Apply A-GPS Data" override the system data, once you click **Submit**. It is therefore advisable to exercise caution using this feature.
- Use Current System Time—Apply the system time currently used by SecureSync for the Survey.
- Set System Time—Enter a specific date and time, instead of the system time. This may be useful if the system time is known to be incorrect, or if you need a time in the past or future, e.g. for simulation purposes. Enter the date and time using the displayed calendar and time sliders.
- Manual Position Set—Clicking this will provide 3 additional fields for the unit's position to be entered manually, or viewed:
  - Latitude, Longitude—in decimal degrees.
  - Altitude—in meters.

### Log entries for A-GPS/A-GNSS

Jul 1 02:15:01 cmc-ntp-01 cmc-ntp-01: [system] No valid A-GPS data from yesterday (CAGPSD)

Jul 1 01:15:01 cmc-ntp-01 cmc-ntp-01: [system] Today's A-GPS data file unavailable from server (CAGPSD)

Starting with software update version 5.1.3, we have added a new feature associated with GPS reception, called Assisted GPS (or "A-GPS"). This new feature allows GPS ephemeris and almanac data to be downloaded from the Internet which is faster than downloading it from the GPS satellites. This feature can help installations with weak GPS signal strengths and speeds up the time it takes for the first positional fix.

**Note:** For more information about A-GPS, refer to websites such as: [http://en.wikipedia.org/wiki/Assisted\\_GPS](http://en.wikipedia.org/wiki/Assisted_GPS).

If A-GPS is enabled, the SecureSync will periodically try to access an Internet site to download this data from a website. These log entries indicate it tried to access this website, but wasn't able to (likely because the time server doesn't have a connection to the Internet).

A-GPS not being able to access the website doesn't adversely affect the operation of the time server in any way. But this function can be disabled as desired to alleviate these log entries from being asserted.

To disable A-GPS, navigate to the **Interfaces** -> **GNSS 0** page of the newer (black/charcoal background) web browser. Click "**edit**" towards the bottom of the page. Towards the center of the pop-up menu (under "A-GPS", de-select "Enable A-GPS" and press Submit. The SecureSync will no longer try to periodically access the Internet. Note that A-GPS cannot be configured via the Classic Interface web browser.

---

### Software Version 4.7L only (Phase 1)

- When the customer has a question about using the SecureSync most of the time the answer will be the same as for any other SecureSync. The exception is for the GPS. Here's the new GPS setup screen:

**Note:** These are for **A-GPS** configuration.

There are four different modes the SecureSync can be placed into for A-GPS operation, including the following:

- A) **No A-GPS** This mode disables the use of A-GPS for the SecureSync. The SecureSync will be in No A-GPS mode by default and is used to turn off or disable the A-GPS feature on the SecureSync.
- B) **Client-SUPL** Skylight One can receive A-GPS data as a client to a SUPL server. A SUPL (Secure User Plane Location) server provides A-GPS data using the SUPL protocol over a network.
- C) **Client-Peer** A Skylight One can also be a client to a second Skylight One configured to be a A-GPS server. The **Client-Peer** mode is used to configure a SecureSync as a client A-GPS device that can connect to a peer server.
- D) **Server** A SecureSync can be configured as an A-GPS server which provides A-GPS data to other SecureSyncs configured as Client-Peer.

**A-GPS configuration (Phase 1 only)**

A-GPS is configured in the **Setup -> Inputs -> GPS** page of the browser (version 4.7L software)

The first 2 tabs have the same content as the regular SecureSync. The A-GPS and Key tabs are specific to Skylight.

**GPS INPUT SETUP**

General Position **A-GPS** Client Key Server Keys

|                |            |
|----------------|------------|
| Receiver Mode  | Standard   |
| Dynamics Mode  | Stationary |
| Offset         | 0 nsec     |
| Position Clear | Disabled   |

Submit Reset

**A-GPS tab**

**GPS INPUT SETUP**

General Position **A-GPS** Client Key Server Keys

|                     |          |
|---------------------|----------|
| Client Server       | A-GPS    |
| Server IP Name      |          |
| Clear A-GPS Data    | Disabled |
| Initialize GPS Time | Disabled |

Submit Reset

**Client Key tab**

**GPS INPUT SETUP**

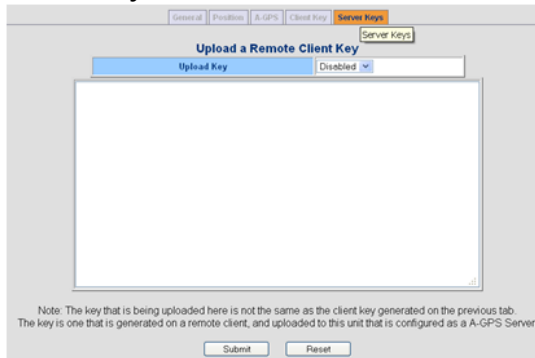
General Position A-GPS **Client Key** Server Keys

|                         |          |
|-------------------------|----------|
| Generate New Client Key | Disabled |
|-------------------------|----------|

Submit Reset



## Server Keys tab

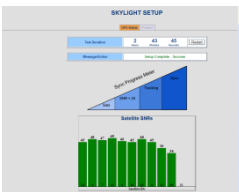


~~New Skylight web page (Never implemented)~~

~~**Notice:** (As of ) this page has NOT yet been made available to the SecureSync. It may someday be added post version 4.7L, But as of now, we are still shipping 4.7L with no immediate plans to release a newer version that incorporates this page.~~

~~**Note:** JavaScript needs to be enabled in web browser for the features on this page to operate! An error message of “your browser does not support scripts” may be displayed, if it’s not currently enabled.~~

~~**Setup -> Skylight** page of the browser: Example Screenshot below~~

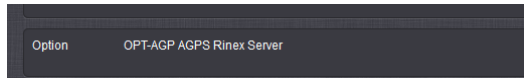


- (GPS Status tab) In the “Message/Action” field (click on “enter UTC offset” if it can’t automatically obtain it right away. This click links over to the Setup -> Time Management page to allow UTC offset to be manually entered. Otherwise, it may take a long time to get this value automatically and SecureSync won’t achieve sync until the value is known (need to manually navigate back).
- In “Position” tab, enter the manual position (just like “single satellite mode”) of the GPS antenna. This tab Links to Google, if they have Internet access.
- “Test Duration” starts when either entering this page or after pressing “Reset” (GPS Status tab).
- SNR bar graph (updates every second)
  - Red = Bad SNR
  - Orange = SNR getting better
  - Yellow = SNR decent
  - Green = SNR good (SNR  $\geq 25$  are considered good signal strengths).
- Automatically recommends relocating GPS antenna after 20 minutes if SNRs  $< 25$  but not in sync OR after 60 minutes if the SNRs  $\geq 25$  and not in sync.
- Should go into Sync with SNRs in the 30s.
- Individual SNR’s update every second. Status bar graph updates every 5 seconds.
- Timing log provides average SNR values.
- GPS Qualification log reports number of satellites that were tracked.

## \*\***(SS-OPT-AGP) A-GPS /AGNSS Rinex Server Option (GPSRINEXD)**

In online user guide at: [http://manuals.spectracom.com/SS/Content/VSS/TIME\\_MGT/VssAGPS.htm?](http://manuals.spectracom.com/SS/Content/VSS/TIME_MGT/VssAGPS.htm?)

- Refer to (Salesforce): <https://na8.salesforce.com/01tC0000004KRDS?srPos=0&srKp=01t>
- Requires Res-SMT-GG (or uBlox with software v5.6.0 or above installed) receiver and “SS-OPT-AGPS” license file be installed (this Option not compatible with Res-T receivers)



### Notes:

- A-GNSS Server RINEX file generation does NOT work with GLONASS. DO NOT ENABLE GLONASS with this feature
- As of software version 5.6.0, this option is now compatible with the newer ublox receivers.
- This Option file can be installed in a new SecureSync before shipment, or in a fielded unit (the SecureSync does not need to be returned for modification, unless it has the earliest Model receiver installed, a Trimble RES-T receiver. This Option is not compatible with this Model receiver, which shipped in SecureSyncs until about Serial Number 5950, Apr 2014.
- This option provides almanac and ephemeris data for GPS and Galileo in RINEX-3 format, via files downloaded from the SecureSync.
- RINEX-3 files (Ephemeris data) are generated in common file/directory structure as the NASA CDDIS site hosting public almanac and ephemeris data files.
- RINEX files can be transferred out using FTP, SFTP or HTTP/HTTPS (web browser) access.
  - The **/pub/gps/data** folder contains three “folders” containing GPS data  
Note the “daily” and “hourly” files are Rinex files (Ephemeris data)

```
spadmin@custservice176 /pub/gps/data $ ls
almanac  daily  hourly
spadmin@custservice176 /pub/gps/data $
```

### Transferring “hourly” files out via the web browser (as an example)

- **Example format below for an hourly file** (where 10.10.128.4 is the IP address of the SecureSync)

**<http://10.10.128.4/files/pub/gps/data/hourly/2015/211/hour2110.15n.Z>**

(IP address, “Hourly” folder, year/day of year/ file name)

```
spadmin@custservice176 /pub/gps/data/hourly/2015/211 $ ls
hour2110.15n.Z
```

**Email from Keith (17 apr 17, per salesforce case 25056)** To begin, the SecureSync’s ASCII Output Option Cards (Models 1204-02 and 1204-04) support three NMEA messages. They are: **GGA**, **RMC** and **ZDA**. They don’t currently support the desired outputs of **ALM** (almanac) or **GSA** (overall satellite data).

However, there is an available SecureSync Assisted-GNSS license file that which be purchased/installed (named “**SS-Opt-AGP**”), which enables RINEX server functionality. Once enabled with a one-time (lifetime license, which doesn’t expire), this option provides almanac and ephemeris data output for GPS and Galileo in RINEX-3 format. The RINEX files can be downloaded out of the SecureSync via an FTP, SFTP or HTTP/HTTPS (web browser) connection.


The GGA NMEA data can be provided (either once-per-second or upon request) via either RS-232 data messages (using the 1204-02 Option Card) or via RS-485 data messages (using the 1204-04 Option Card).

Hongbo can provide you with the cost to purchase the SS-Opt-AGP license file. Note this Option file can be installed in a new SecureSync before shipment, or in a fielded unit (the SecureSync does not need to be returned for modification, unless it has the earliest Model receiver installed, a Trimble RES-T receiver. This Option is not compatible with this Model receiver, which shipped in SecureSyncs until about Serial Number 5950, Apr 2014.

**Details of SS-Opt-AGP operation (email in red from Paul Myers, 20 Apr 17)**

**Important Note: Can't have GLONASS enabled when AGPS server is enabled**

**Per the online user guide**

 **Caution:** Do NOT use GLONASS when operating SecureSync as an A-GNSS server, since this will likely crash the A-GNSS software.

- Glonass being enabled can crash the Rinex server option i
- The following System log entries are assertedL
  - Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
  - Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)

The OPT-AGP if a u-blox M8T receiver is installed or Trimble RES-SMT GG receiver is installed provides the function of a A-GPS server. An A-GPS server allows the collection of RINEX3 formatted Navigation files and GPS Almanac files.

If a multi-GNSS licenses OPT-GNS is installed the u-blox M8T acts as an A-GNSS server by allowing the user to select Galileo and or BeiDou as well allowing the collection of RINEX3 navigation files and Almanac files for the GPS, Galileo and/or BeiDou constellations. At this time the GLONASS constellation is NOT supported. GLONASS should not be enabled as it causes the feature to not operate at this time.

The user can navigate to the Interfaces -> GNSS 0 web page and select "Edit"

At the bottom of the Edit panel the user can enable "Generate Rinex/Yuma Files"

For u-blox M8T you can select when YUMA Almanac files are created, the Station Name 4 character prefix and the number of days at which the Almanac/RINEX3 files are preserved.

You can specify whether an Almanac file is created once per day or updated at a specific number of seconds intervals.



Generating Almanac every 300 sec.



The files can be remotely accessed via /pub path on the SecureSync or via the mapped

Note the Trimble RES-SMT GG receivers can specify how often the RINEX3 data is updated. This is not needed for the u-blox M8T as the data is updated on change.

A-GPS

Enable A-GPS Client

Generate Rinex/Yuma Files

Rinex File Every: 10 s

Generate Yuma once a day

Yuma File Every: 300 s

Station Name: spec

Record Duration: 90 d

Status Submit

### Issues associated w/Rinex Server option enabled

- 1) **A-GNSS Server RINEX file generation does NOT work with GLONASS.**
- 2) **DO NOT ENABLE GLONASS with this feature**
- 3) **System log contains Failed to read Almanac from GPS receiver (GPSRINEXD) and Failed to read Almanac from GPS receiver (GPSRINEXD) entries**

➤ Refer to SF case 121361

➤ Caused by having Glonass constellation enabled in the list of receiver constellations enabled.

```
Nov 7 19:33:54 Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
Nov 7 19:34:00 Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)
Nov 7 19:34:04 Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
Nov 7 19:34:10 Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)
Nov 7 19:34:14 Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
Nov 7 19:34:20 Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)
Nov 7 19:34:24 Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
Nov 7 19:34:30 Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)
Nov 7 19:34:34 Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
Nov 7 19:34:40 Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)
Nov 7 19:34:44 Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
Nov 7 19:34:50 Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)
Nov 7 19:34:54 Spectracom Spectracom: [system] Failed to read Ionosphere from GPS receiver (GPSRINEXD)
Nov 7 19:35:00 Spectracom Spectracom: [system] Failed to read Almanac from GPS receiver (GPSRINEXD)
```

### Fix:

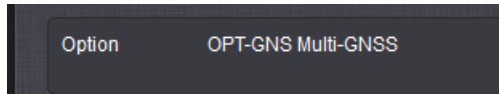
➤ Make sure the Res-SMT-GG or ublox (v5.6.0 and above only) receiver is configured with GLONASS disabled,

---

## \*\***(SS OPT-SKY) Skylight Option**

### **Opt-SKY/Skylight (SecureSync with indoor antenna and Res-SMT receiver)**

#### **C) (SS OPT-GNS Multi-GNSS) GNSS receiver/GNSS receiver upgrade (Glonass L1 1602 MHz)**



**Note:** version 5.7.0 (Jun 2017) alleviates the need to purchase this license if its desired to add additional constellations beyond just GPS. Once a unit has been updated to 5.7.0 or above, the unit has the ability to enable GPS and other satellite constellations (units with just GPS before updating will just have GPS enabled after updating. But they can then go in and enable other constellations if desires.

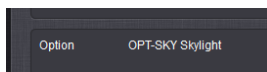
- Our P/N: "SS OPT-GNS"
- Purchased option for SecureSyncs
- Not applicable to SAASM units
- Requires either RES-SMT-GG or u-blox M8T (compatible with software versions 5.4.1 and above) be installed.
  - Can be applied in field via purchased license file with Res-SMT-GG receiver installed (started shipping ~1 Apr 2014)
  - Can be used with Model 8230 GNSS antenna (Model 8225 GPS antenna needs to be replaced with a Model 8230 GPS/GNSS antenna)
- Refer to the GPS/Glonass info in this document for more info
- Refer to the following page for pricing and additional information  
<https://na8.salesforce.com/01tC0000003IGr1?srPos=4&srKp=01thttps://na8.salesforce.com/01tC0000003IGr1?srPos=4&srKp=01t>
- The Cost to upgrade from a commercial Res-T GPS receiver to RES-SMT-GG Glonass receiver - refer to the Repair excel worksheet at: [repair info.xlsx](#)

#### **Galileo constellation**

- Requires ublox receiver with firmware version 3.0.1 or above be installed (we started receiving v3.0.1 in ublox receivers ~Nov, 2016).

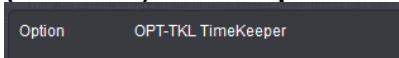
---

#### **D) (OPT-SKY) Skylight phase 2**



---

#### **E) (OPT-TKL) Timekeeper**



**F)  
G)**

---

#### **H) (Opt-PD1) Peer Daemon Option**

- Started with the 'Triggerfish' special (refer to "Specials" below for more info on this option).
- The Peer Daemon allows two SecureSync's to act as NTP Servers to communicate when NOT using a Primary Reference like GPS and determine which is the best and should be NTP Stratum 1.

---

#### **I) (Opt-SEM) Option SAASM Emulation**

- Refer to: [Opt-SEM \(Option SAASM Modulation\)/ Time Mark Data Message \(ID 3\)](#)

## Replacing discontinued Rapco Models 1804/2804 with SecureSync

- SecureSyncs can be used to replace the discontinued Model 1804s and Model 2804s
- Refer to Salesforce Cases such as 202640

### ***Rapco Models 1804/2804 discontinuance letter***



Orolia USA, Inc.  
1565 Jefferson Road  
Suite 450  
Rochester, NY 14623 USA  
Tel: +1 585.321.5800  
Fax: +1 585.321.5219  
www.spectracomcorp.com

#### SPECTRACOM PRODUCT DISCONTINUANCE NOTICE

**Product:** Rapco 1804 and 2804 Master Clocks and 2816 Tracking Oscillator

**Effectivity Date:** April 24, 2013

**Final Order Date:** June 30, 2013

**Replacement Product:** SecureSync

Rapco family of GPS masterclocks, including models 1804 and 2804 and tracking oscillator model 2816, is nearing end-of-life. It has been replaced by SecureSync model, which offers unsurpassed modularity and performance, as well as many improved features and functionality. Still, last-time buy orders for the models 1804, 2804 and 2816 will be accepted by June 30, 2013, for delivery on or before December 30, 2013.

Standard support for the 1804, 2804 and 2816 models via hardware repairs is expected to be available up to 2018. Limited software support will be provided up to 2015. For support beyond these dates, specific support contracts can be setup upon request.

## **\*\*SS-OPT-TKL Timekeeper Options for NTP/PTP**

- **Our P/N:** OPT-TKL (I believe)
- Adds Timekeeper NTP/PTP monitoring
- Timekeeper software started being installed in SecureSync with the version 5.2.0 software update (Jan 2015)
- Can be applied in field via purchased license file
- First version of timekeeper installed in SecureSync- version 7.0.6.

**Note:** for all the details, refer to: [\\*\\*OPT-TKL \(Timekeeper software in SecureSync\)](#)

**Notice:** (As of at least Dec, 17) Timekeeper option is not compatible with the newer variant ETX module. I don't anticipate it will ever be compatible.

## Removal of Broadshield and Timekeeper software from existing 5.8.4/5.8.5 (and future) SecureSync upgrade bundles (for both Options to be removed from units, when the bundles are obtained from us after 10 Sept 2019)

- Refer to ECO-FAI-2269 (in Arena): [https://app.bom.com/changes/detail-summary?change\\_id=2397735912&](https://app.bom.com/changes/detail-summary?change_id=2397735912&)
- Title of ECO: **"SecureSync 5.8.4 / 5.8.5 - Remove Timekeeper/Broadshield from software"**
  - **Effective date:** 10 Sept 2019

---

## Special software patches / Specials for SecureSync

### Special software patches for particular or all customers:

#### 1. CF Card healthcheck patch: CF card write usage/expected life expectancy patch (“ss\_healthcheck.tar.gz”)

- In all SecureSyncs/9400s starting in **update version 5.8.5**
- Refer to “CF card write usage/expected life expectancy patch (“ss\_healthcheck.tar.gz”)” in the Compact Flash Card section of this document for more info

---

#### 2. “updateGb3421.tar.gz”: v5.8.4 NTP Improvements patch (for Morgan Stanley)

- Refer to Salesforce Case case Number 170655
- Refer to [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software\\_patches](I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software_patches)
- This patch was added to main software trunk in **version 5.8.5** (versions **5.8.6 and above** inherently have this newer driver already installed)
  - **From v5.9.4 kern.log without patch being applied:** “e1000e: Intel(R) PRO/1000 Network Driver - 3.4.2.1-SPEC”

**Purpose of this patch (for update versions 5.8.5 and below only):** Improves restarting of the network processors when there is heavy traffic (“RNBC” counters, reported in the **System** log)

#### Verification of successful patch install:

**Email from Ron Dries to Dave L (5 March 2019)** the new patch **updates the e1000e** driver. It should report as 3.4.2.1 in the kern.log. Things to check are the system.log and update.log to make sure there are no errors, Then the kern.log to make sure the e1000e driver is the correct version: **3.4.2.1-SPEC** (example: “e1000e: Intel(R) PRO/1000 Network Driver - 3.4.2.1-SPEC”)

**Except from Salesforce Case 170655, listing their initial observations (for which this patch was developed)**

1. Under NTP req testing, CPU utilisation has gone from 59% (v5.7.1) to ~85% (v5.8.1).
2. Timing offset tests seen from Timekeeper server has gone from ~15us max drift (v5.7.1) to ~27us max drift (v5.8.1).
3. Timing RAW offset tests seen from Timekeeper server has gone from ~40us max drift (v5.7.1) to ~1500us max drift (v5.8.1).
4. Under NTP req testing, **timing** offset tests seen from Timekeeper server has gone from ~40us max drift
5. (v5.7.1) to ~250us max drift (v5.8.1).

#### **Email from Sadie Nedo (5 March 2019)**

FYI: Dave Sohn and I delivered this patch to Morgan Stanley this week. It addresses port flapping and timing performance issues raised by Ravi. Attached is an in-depth report.

- The latest SecureSync SW is here: <https://files.spectracom.com/public-downloads/latest-securesync-netclock-files>
- The patch for the network driver is here: <https://files.spectracom.com/client-downloads/6245>
- The patch needs to be applied after they upgrade to the 5.8.4 SW.

This was sent to Ravi Kambo, Erhan Senlik, and Constantine “Gus” Paleatsos.

This is in response to Ravi’s open case # 170655.

---

#### 3. e1000e patch to change the port speed from 333 usecs to 50 usecs (for Morgan Stanley)

- Refer to Salesforce Case 25619

Refer to patch info in: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software\\_patches\Morgan Stanley e1000e patch](..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software_patches\Morgan Stanley e1000e patch)

**Except from Salesforce Case 25619, listing their observations (which this patch was developed for)**

NY4 and NY5 have about a 100uS timing discrepancy as indicated in Carteret site.

NY4 sf01pdmi34 running Timekeeper is different than NY5 nj01pdmi107. Serving time the Exegy Market data computer in Carteret and the timing is 100uS different between the two.

#### Verifying this patch is installed

**Email from Dave L (5 March 2019)** “...E1000E patch Ron Dries made for them last summer to change the port speed from 333 usecs to 50 usecs and can check to see if it was applied using the same CLI commands.”

```
ethtool -c eth1 | grep rx-usecs:
```

**Note:** This e1000e patch (available for 5.8.2, or included in 5.8.3 and above) being installed can cause SecureSync to inadvertently go into Holdover mode, with heavy NTP request loading. Refer to more info in this document “*\*\*\*Issues with NTP Stratum synchronization*”

---

#### 4. updateRbDisc.tar.gz”: Patch to remove KTS disciplining of a Rubidium oscillator

- LPN Rb and Standard Rubidium oscillator disciplining/need to apply a special EPROM patch (“**updateRbDisc.tar.gz**”) patch when downgrading software version
- Due to a change to newer method of RB oscillator disciplining starting in 5.8.0 (KTS disciplining the oscillator), a special EPROM patch (“**updateRbDisc.tar.gz**”) file needs to be applied to switch the Rb oscillator to start using the earlier method of disciplining (its own internal disciplining). Until the patch is applied, the oscillator will remain always in a free-run state.
  - **Link to updateRbDisc.tar.gz:** [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Downgrade Rb patch \(updateRbDisc.tar.gz\)](I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Downgrade Rb patch (updateRbDisc.tar.gz))

**Important Note:** Installing this patch on unit not having a Rb oscillator installed (such as TCXO/OCXO) has been shown to corrupt the EPROM (not fixed with a standard upgrade/downgrade) a special patch to restore the EPROM back to the original configuration has to be applied in the field or at the factory.

- **Refer to:** [I:\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Downgrade Rb patch \(updateRbDisc.tar.gz\)\patch installed on tcxo-ocxo](I:\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Downgrade Rb patch (updateRbDisc.tar.gz)\patch installed on tcxo-ocxo)

---

#### STANDARD RB (not LPN RB) oscillator disciplining with versions 5.7.1 and below VERSUS verions 5.8.0 and above

##### A) Software versions 5.8.0 and above

- software changed from Rb disciplining itself to using the same algorithm as OCXO/TCO (KTS disciplining)
  - **(5.8.0 and above) “xo1” now being annotated in Rb osc log entries:** Rb is disciplined using KTS (ike OCXO and TCXO log entries have always been)
  - Example entry below with KTS disciplining (v5.8.0 and above installed)

[system] 2015 170 07:11:04 000 **XO1**: Frequency error recalculated: -00.000332 (-3.328x10<sup>-12</sup>)

---

##### B) Software versions 5.7.1 and below

- “xos” was annotated in Rb osc log entries = indicates original disciplining (Rb disciplines itself in 5.7.x and below)
  - Example entry with Rb disciplining itself from (v5.7.x and below)

[system] 2018 119 15:56:13 000 **XOS**: Frequency error recalculated: -00.000005 (-5.194x10<sup>-13</sup>)



## Downgrading a Rubidium unit from versions 5.8.0 (or above) back to 5.7.1 or below (newer disciplining algorithms back to original disciplining)/need to install the rb patch

- Refer to Salesforce Case 180207
- Its **not** recommended to downgrade Rb units back to 5.7.x or below, once they are at a more recent version.
- but if the software is downgraded and a Rb is installed, a special patch file has to be installed- to switch the EPROM back to the original disciplining
- symptoms of downgrading software without the patch being applied includes TFOM values higher than expected (oscillator will be in constant free-run).
- in case 180207, algorithms changed correctly going forward from 5.7 to 5.8.2 But the EEPROM does not change back to the original disciplining of the Rb, when its downgraded (the oscillator stayed with the new method, but the earlier version of software stayed) -so the oscillator wasn't properly disciplining after the downgradd. It was instead ramping off.
- To downgrade the disciplining back to the "Rubidium internally disciplining itself" requires the EEPROM be reprogrammed at the factory (in the field- EEPROM can go forward to KTS disciplining but it cant go back to the Rb disciplining itself once its using KTS disciplining-until the patch is applied)
  - This patch file (and draft email) is located at: [..\\.\\EQUIPMENT\\SPECTRACOM\\EQUIPMENT\\SecureSync\\Oscillators, rb material\\oscillator disciplining\\downgrade Rb patch](file://.\\.\\EQUIPMENT\\SPECTRACOM\\EQUIPMENT\\SecureSync\\Oscillators_rb\\material\\oscillator%20disciplining\\downgrade%20Rb%20patch)

---

## 5. Delay GPS sync upon initial boot-up (for EF Johnson/DFW Airport)

- refer to Salesforce cases for Richard Smith (such as 171474 175607)
- Refer to patch info in: [\\rocfnp02\\drive\\Customer Service\\EQUIPMENT\\SPECTRACOM\\EQUIPMENT\\SecureSync\\Specials\\software patches\\](file://rocfnp02\\drive\\Customer%20Service\\EQUIPMENT\\SPECTRACOM\\EQUIPMENT\\SecureSync\\Specials\\software%20patches)

**email from Dave L (after he spoke to Dave Sohn) 21 Dec 2018** From speaking with engineering I believe that you must first disable the GNSS 0 Reference in the Reference Priority table so the system starts up with no GPS input, then enables it automatically after startup. Can you check the refence priority table and see how it is configured? Otherwise we should probably CLEAN the configurations and reload. There may be an issue loading your configuration file. Was the config file saved from a version 5.7.X unit.

---

## 6. Disable IRIG output on startup (for LMCO)

- Refer to patch in: [.\\Customer Service\\EQUIPMENT\\SPECTRACOM\\EQUIPMENT\\SecureSync\\Specials\\software patches\\Disable IRIG on Startup](file://.\\Customer%20Service\\EQUIPMENT\\SPECTRACOM\\EQUIPMENT\\SecureSync\\Specials\\software%20patches\\Disable%20IRIG%20on%20Startup)

### Notes about this patch

- Restoring a config bundle downloaded from a "non-patched" unit will remove the patch from a previously patched unit.
- Per Ron, this patch initially disables all input references in in the Reference Priority table until the kts.if file is read after power-up.

**email from Ron Dries (10 aug 18)** Here is a link to download the patch for LMCO to disable IRIG output on startup: <https://files.spectracom.com/client-downloads/5965>

This update patch is only applicable to 5.7.0 software versions. If the patch is applied to a non-5.7.0 SecureSync the following message will appear in the update log: "Problem running runbefore.sh (SWUE)"

This patch does not change the NWP software version so it will report a failure after reboot, however the KTS (timing system) version will be 3.4.G if it has been applied.

After the patch has been applied and the SecureSync reboots the IRIG outputs will be disabled. The user will have to go in and manually set signature control back to on.

When this is done on subsequent reboots the output will be off until the system reaches a point in the startup process where it applies user timing system configuration changes. At this point the IRIG output will then start outputting again.

If a clean update to 5.7.0 is performed this patch will need to be applied, otherwise the timing system will remain untouched. If they update to a version other than 5.7.0 the patch will no longer be applicable.

Performing a clean, or configuration restore will not impact the default signature control change, however the user signature control changes will be impacted.

---

## 7. Disable redundant input power alarm (for T-Mobile)

- Refer to associated case **183632** for info below (this isn't the original case, but one submitted sometime after they received the patch discussed below)
- **Report for case 183632:** We fixed the Snapshot problems when launching these devices on our network w/ the software upgrade you provided (lockfile issue fixed). We are now experiencing failed snapshots again for the same reason and we need help!

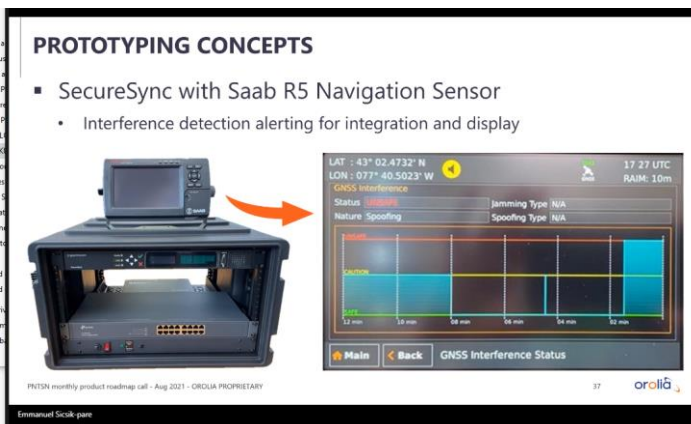
**email from Sadie (16 Jan 2019)** He's talking about a patch that Ron made. They have Dual powered appliances but only connect one power to the devices, so there was an alarm showing a disconnected power input. Ron created a patch that changes the configuration to single power to suppress the alarm (I think).

- Refer to patch in: [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software\\_patches\Disable Power fault with dual input power](#)

## SPECIALS/Prototypes

### A) SPC-MSS-SR5: SecureSync with Saab R5 Navigation Sensor (IDM sensor)

- Apps team (Especially Ron Dries) working for commercial Maritime ships' ability to detect GPS jamming/spoofing,
- 1st order (SO 93305) shipped 14 Oct 2021.
- **Model:** M-SecureSync RPNT with Saab R5
- **P/N:** SPC-MSS-SR5
  - **In Arena:** [https://app.bom.com/items/detail-spec?item\\_id=1299767165&version\\_id=11993041208&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1299767165&version_id=11993041208&orb_msg_single_search_p=1)



## BOM

- Consists of (1)SecureSync 1200-003 with Opt-SS-BSH, (1)1204-02 and (1)1204-04 Option Cards
  - Option Cards send Jam/Spoof info via ASCII messages to other equipment.
- Refer to spreadsheet (in Arena) at: [https://app.bom.com/items/detail-spec?item\\_id=1299767165&version\\_id=11993041208&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1299767165&version_id=11993041208&orb_msg_single_search_p=1)

| 1                     | 2                                                                                                               | 3        | 4                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------|
| Part Number           | Description                                                                                                     | Quantity | Link                                                                          |
| 1200-003              | SecureSync Model 1200-003                                                                                       | 1        | Orolia Product                                                                |
| 1204-02               | SecureSync ASCII Time Code In/Out [RS-232] Option Card                                                          | 1        | Orolia Product                                                                |
| 1204-04               | SecureSync ASCII Time Code In/Out [RS-485] Option Card                                                          | 1        | Orolia Product                                                                |
| CA06R-1513-0001       | Power Cord, AC, North America Plug                                                                              | 1        | Orolia Product                                                                |
| PE9090                | TNC to N adapter                                                                                                | 1        | <a href="#">N Male to TNC Female Adapter (pasternack.com)</a>                 |
| MP01R-0003-0010       | Portable Roto Molded 6U Rack                                                                                    | 1        | Orolia Product                                                                |
| MP01R-1U00-0004       | Rackmount Power Strip - 8 Rear outlets with 90° turn                                                            | 1        | Orolia Product                                                                |
| MP01R-1U00-0005       | 19" 1U 10" Deep - Half Shelf - 2 post                                                                           | 1        | Orolia Product                                                                |
| 8224-21050            | GNSS Splitter 1:2                                                                                               | 1        | Orolia Product                                                                |
| 8224-41050            | GNSS Splitter 1:4                                                                                               | 1        | Orolia Product                                                                |
| CS-201GII             | DAIWA CS-201GII COAX SWITCH N CONNECTORS - 2 GHZ                                                                | 1        | <a href="#">Daiwa - Daiwa CS-201GII Coax Switch N Connectors - 2 GHz #451</a> |
| ADD050SLOGPRO         | AirDrive Serial Logger Pro - RS232 Logger and Data Recorder with WiFi, 16GB Flash, Email and Live Data Transfer | 1        | <a href="#">Serial data recorder - AirDrive Serial Logger (keelog.com)</a>    |
| PI4-2GB-STR32F-C4-BLK | Raspberry Pi 4 Starter Kit 2Gb (4Gb \$99.98)                                                                    | 1        | <a href="#">Raspberry Pi 4 Starter Kit (canakit.com)</a>                      |
| 8230AJ                | 8230 AJ Antenna                                                                                                 | 1        | Orolia Product                                                                |
| 8226                  | Surge Protector                                                                                                 | 1        | Orolia Product                                                                |
| Antenna-Suction-Mount | TechnoRV Suction Cup Antenna Mount                                                                              | 1        | <a href="#">Suction Cup Antenna Mount (technorv.com)</a>                      |
| MP32R-0002-0002       | 16-Port Gigabit Desktop/Rackmount Switch                                                                        | 1        | Orolia Product                                                                |
| 19                    |                                                                                                                 |          |                                                                               |
| 20                    |                                                                                                                 |          |                                                                               |

### B) "SecureSync 233, Embraer"

This is a special version of Securesync designed to work on the Embraer E-99 P/N.

- Special SecureSync 1200-233 for "EMBRAER AVIATION INTERNATIONAL"
- **Spectracom P/N:** 1200-9079-0601 (consists of 1200-233, 25,1C with a Wenzel Ruggedized Oscillator.)
- Refer to (Salesforce Opportunities): <https://orolia.my.salesforce.com/0060h000017DWrv?srPos=0&srKp=006>
- Contains Wentzel oscillator for very low 1MHz phase noise output
- Designed at Les Ulis O2S, but apparently not controlled/classified in any way???

**\*\*\*\*10 MHz output Signature Control**

**(11 March 2020) Note about SecureSync LPN Specials having a Wentzel oscillator installed, such as the SPECIAL Clock Generation Unit (CGU) for Hughes**

- Apparently, due to design changes needing to be incorporated to add the Wentzel LPN oscillator, 10MHz Signature Control is still displayed in the web browser. But it's not functional.

**Email from Dave L (11 March 2020)** This is confirmed to be a limitation of the product design. Incorporating the low phase noise oscillator feature has disabled the Signature Control function.

**C) "037 SS SAASM GSA Kit" (Top level part for the Testmart GSA kit)**

- P/N 1200-9065-0700 (in Arena): [https://app.bom.com/items/detail-spec?item\\_id=1258567198&version\\_id=11254235778](https://app.bom.com/items/detail-spec?item_id=1258567198&version_id=11254235778)

1200-9075-0601: **GSA Testmart kit which includes a SecureSync 037 with option cards 13, 06, 15, and 1A. Kit also includes cables and Model 8225S antenna.**

**D) QEWR Special (SecureSync-057 in 20 inch chassis, 5 MHz outputs via Option Card)**

- Refer to: <U:\Engineering\Projects\QEWR>
- Refer to ECOs (in Arena) such as 1707
- SecureSync 057,18,46,27,1E,1A,00 (1200-9022-0500) in a 20 inch chassis
- Wentzel oscillator VNDA-4-5-2-2-1 Distribution (1771-1818) and a separate Wentzel component next to the oscillator  
1204-46 Option Card provides four (4) 5 MHz outputs

**E) BCFAO Special (SecureSync-233 w/VersaSync AM IRIG Option Card)**

**F) Special carrier board for ublox M8T receiver/special software (+12vdc output to GNSS antenna)**

- Refer to ECOs: ECO-1852, ECO-1760 and ECO-1770 in Arena
- This board will support a 12V antenna supply
- This board does not support short circuit detection. It does support open antenna.
- **SecureSync 233, TE622/SL5M Replacement:** 1200-9055-0601 (in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1253488729&version\\_id=11134592028&](https://app.bom.com/items/detail-spec?item_id=1253488729&version_id=11134592028&))

This special is a standard SecureSync with a customer Rb with one of its pins configured to output a 0-5V "LOCK" status. This pin will be wired to a DB25 connector that is installed on the new "4F" option plate. This unit will also have custom software that is based on the 5.8.1 release.

This special also uses a new U-Blox carrier board that uses +12v for the antenna.

---

## G) SecureSync Special for NEC – PTP

- Special SecureSync for NEC - PTP Upgrade for Army.
- Refer to ECO-1748 in Arena: [https://app.bom.com/changes/detail-summary?change\\_id=2394092759&](https://app.bom.com/changes/detail-summary?change_id=2394092759&)
  - 1200-033
  - 1204-32
  - 1204-3B
  - 1204-01

Since the 1204-3B, PTP Slave card is still released as a Special, engineering will be responsible for testing the "3B" option card.

Option cards must be installed as shown per customer request.

Had to withdraw and update BOM. See customer request below:

Per an email from Joshua: The customer only needs 1x SFP-COPPER module installed in the -32 card.

Apparently they have run tests with the module in -3B card and it failed so they will be supplying their own alternative. Please update the BOM to include only 1x SFP-COPPER. Thanks.

---

## H) Triggerfish - (Opt-PD1) Peer Daemon Option

- For more info, refer to ECO-item-000824 in Arena: [https://app.bom.com/changes/detail-summary?change\\_id=2386135570&](https://app.bom.com/changes/detail-summary?change_id=2386135570&)
- Refer also to: <U:\Engineering\Projects\Triggerfish>
- The Peer Daemon allows two SecureSync's to act as NTP Servers to communicate when NOT using a Primary Reference like GPS and determine which is the best and should be NTP Stratum 1.
- This change is intended to document the Triggerfish Special SecureSync/NetClock 94XX Release 5.4.3 KTS 3.3.4 which introduces the Peer Daemon. The Peer Daemon allows 2 SecureSync's to act as NTP Servers to communicate when NOT using a Primary Reference like GPS and determine which is the best and should be NTP Stratum 1
- Quantity=(2) SecureSync 1200-1271-0601 with 1204-06 cards (Serial Numbers 11784 and 11785)
- No GPS receiver
- Software version 5.4.3/KTS version 3.3.4
- License OPT-PD1 Peer Daemon Option for each Unit
- See Paul Myers for support with this special.

### software updates associated with Peer Deamon

**Per Paul Myers (24 May 16) Implemented or FIXED in Release 5.4.3 KTS 3.3.4 (TRIGGERFISH)**

|                    |                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>     | 0003243: Ethernet Monitor: two Graphs display data but "Download monitoring data" results in empty excel spreadsheet                                                                                                        |
| <b>Description</b> | (Not positive this is a software bug, but it's something I happened to observe)<br>The two graphs in the System Monitor page are full of data but the "Download monitoring data" button results in empty excel spreadsheet. |

---

## I) 3DLLR Special (3 dealer) (Also referred to as "Raytheon C-Band Radar Unit") (SecureSync 1200C-R477)

➤ **P/Ns:**

- **1200-R009-0601** (SAASM receiver installed) (in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1219866509&version\\_id=10661322848&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1219866509&version_id=10661322848&orb_msg_single_search_p=1))

and

- **1200-9002-0601** (SAASM receiver not installed)

- For more info, refer to ECO-item-00037 in Arena [https://app.bom.com/changes/detail-summary?change\\_id=2386152977&](https://app.bom.com/changes/detail-summary?change_id=2386152977&)
- Refer also to: [U:\Engineering\Projects\RCBR \(3DELRR\)](U:\Engineering\Projects\RCBR (3DELRR))
- P/N for Process Detail: 1200C-R477-0600-PD
- 24VDC input
- Modified SAASM (GB-Gram) -SecureSyncs for Raytheon/SAIC
- Wentzel 10 MHz oscillator (Our P/N Y100R-0002-PC03) for very low phase noise with shock/vibe.
- Conformal coating of PCB and ruggedization of components.
- See Tim Tetreault for any specifics regarding this special SecureSync master oscillator.
- Software version 5.4.4.
- I believe this unit has Opt-SEM installed/enabled (see info below):

**Link to Block diagram (in U drive)** : \\rocuso.uso.oroiausa.com\us-only\Engineering\Projects\RCBR (3DELRR)\1\_Project folder\200 Engineering Documents\Block Diagram

**\*10 MHz output Signature Control**

**(11 March 2020) Note about SecureSync LPN Specials having a Wentzel oscillator installed, such as the SPECIAL Clock Generation Unit (CGU) for Hughes**

- Apparently, due to design changes needing to be incorporated to add the Wentzel LPN oscillator, 10MHz Signature Control is still displayed in the web browser. But it's not functional.

**Email from Dave L (11 March 2020)** This is confirmed to be a limitation of the product design. Incorporating the low phase noise oscillator feature has disabled the Signature Control function.

**(Opt-SEM) Option SAASM Emulation**

- My understanding from Paul Myers is this unit has Opt-SEM installed/Enabled
- This was a special config for them. But its also available as an option for others w/SAASM receiver installed
- Refer to: [Opt-SEM \(Option SAASM Modulation\)/ Time Mark Data Message \(ID 3\)](#)

---

**J) eLORAN (Opt EL1)**

- Special for Rhode and Schwartz (Les Ulis customer)
- Software verson 5.4.2 (based on version 5.4.1)

---

**K) 1200 LPN, g-Compensated Oscillator SecureSync for Raytheon (SecureSync R563)**

- See Tim Tetreault for any specifics regarding this special SecureSync master oscillator.
- Our P/N: **1200-R007-0601** (SecureSync R563,15,06,15,12,15,00)

- Dec, 2014 time-frame
- Refer to ECO-000164 ([https://app.bom.com/changes/detail-summary?change\\_id=2384301368](https://app.bom.com/changes/detail-summary?change_id=2384301368))
- Low phase noise 10 MHz in a high G environment on ship (using an internal SpectraTime SRO-100 Rb oscillator and a Morian external 10 MHz OCXO oscillator that is specialized for High G's (details for this oscillator below):
  - **Mfg/P/N:** Morian X001151M (I believe this is a custom oscillator)
  - **Our P/N:** Y100R-0002-PH09
  - **Our Spec sheet:**  
<https://files.bom.com/download/tbvAbexlHEgxf4dhx2u5EEJfjz9mWz1z/xrpajljoubsimkfwogqxfhygszqrbfub/Y100R-0002-PH09%20SCD%20Rev%20C.pdf>

### **Lock status indicator for the external OCXO oscillator**

- Software version 5.2.0 (~Jan 2015) is adding an indication in the browser for the lock status of the external OCXO oscillator. The mechanical requirements for this indicator are already in place since first one shipped. Just need this software update for them to be able to use it.

---

### **\*\*\*\*10 MHz output Signature Control**

#### **(11 March 2020) Note about SecureSync LPN Specials having a Wentzel oscillator installed, such as the SPECIAL Clock Generation Unit (CGU) for Hughes**

- Apparently, due to design changes needing to be incorporated to add the Wentzel LPN oscillator, 10MHz Signature Control is still displayed in the web browser. But it's not functional.

**Email from Dave L (11 March 2020)** This is confirmed to be a limitation of the product design. Incorporating the low phase noise oscillator feature has disabled the Signature Control function.

---

## L) Hughes Clock Generation Unit (CGU): (SecureSync with very low 10 MHz output phase noise)

- “SecureSync 1200-CGU 1505499-0001” (SecureSync C073,38,00,0D,00,15,00 and a separate distribution chassis)
- Refer to the CGU manual addendum for Hughes (1200-5000-C050) in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1217182411&version\\_id=10446313248&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1217182411&version_id=10446313248&orb_msg_single_search_p=1)

**Note:** the SecureSync is referred to as the “MRO” in this document (MRO-1 and MRO-2 are the 10 MHz outputs from the SecureSync used for the PLL generation)

- See Engineering (Tim Tetreault) for any support requirements related to the product.
- Refer to ECO-0554 for more details (Sept 2015) [https://app.bom.com/changes/detail-affected?change\\_id=2385245472&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/changes/detail-affected?change_id=2385245472&orb_msg_single_search_p=1)
- Refer also to: <U:\Engineering\Projects\Hughes CGU Special>

### Summary

- This special for Hughes consists of two separate devices:
- a SecureSync with a Wentzel 10 MHz oscillator installed for very low phase noise (note the Wentzel osc is the primary/only 10 MHz oscillator in this special- its not a secondary oscillator receiving a 10MHz input from another Primary oscillator co-installed in the chassis, as is the case in some other specials).
- a “Forward and Return Distribution chassis” (FRU) device from Wentzel, which Hughes interfaces together locally using cables which we supply in the anc kit
- The SecureSync provides the FRU with one (or possibly two-see note below) very low phase 10 MHz output(s),
- The FRU locks two PLLs to two 10 MHz inputs (provides eight 112 MHz outputs and eight 140 MHz outputs)

### (11 March 2020) Note about SecureSync LPN Specials having a Wentzel oscillator installed, such as the SPECIAL Clock Generation Unit (CGU) for Hughes

- Apparently, due to design changes needing to be incorporated to add the Wentzel LPN oscillator, 10MHz Signature Control is still displayed in the web browser. But it's not functional.

**Email from Dave L (11 March 2020)** This is confirmed to be a limitation of the product design. Incorporating the low phase noise oscillator feature has disabled the Signature Control function.

**Note:** the original Hughes intention was for the SecureSync to provide only one of the two 10 MHz inputs on the FRU (to lock only one of the two PLLs). The second 10 MHz input for the other PLL was to be supplied from a non-Spectracom source. But its up to Hughes whether they provide 10 MHz from two different sources, or both 10 MHz be supplied by two separate outputs from the same SecureSync.



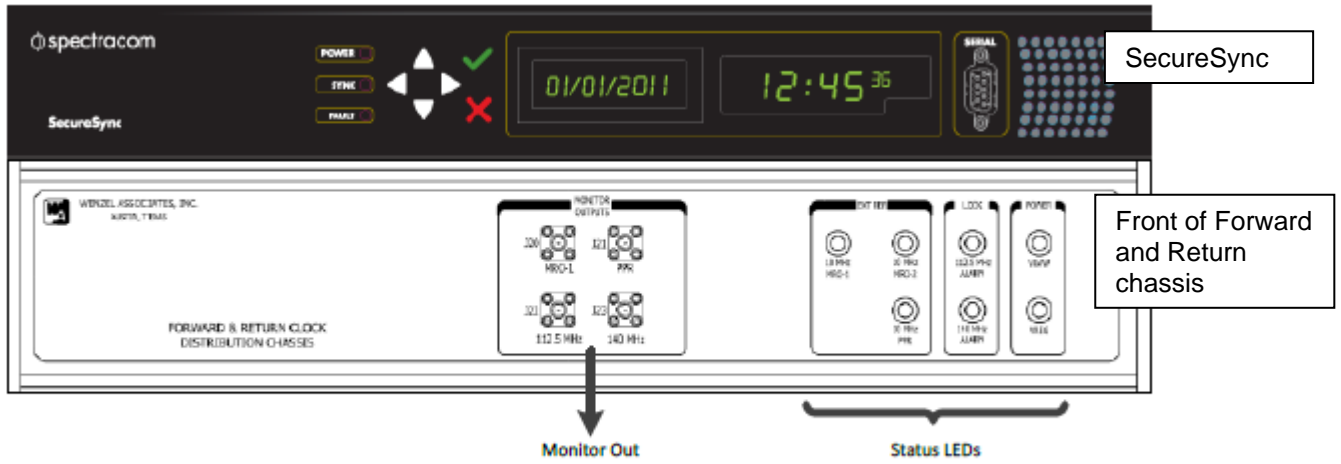
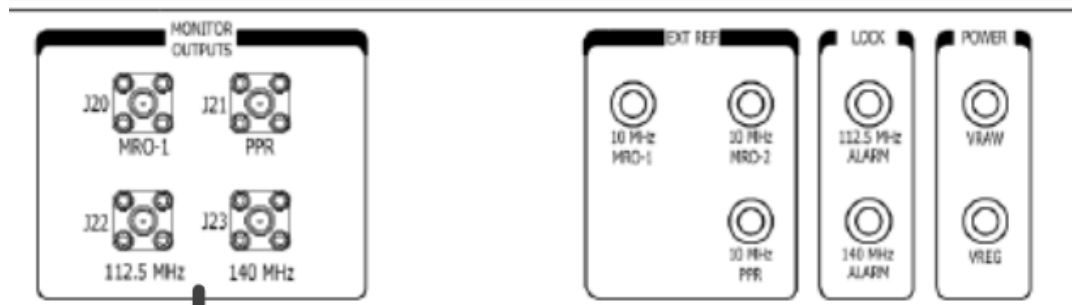
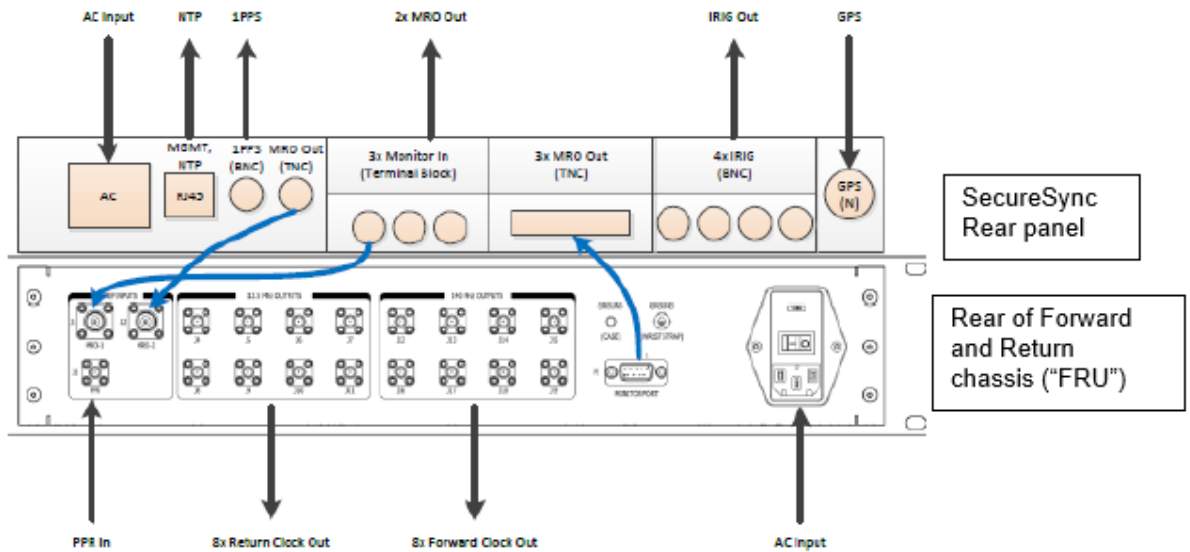


Figure 1 - Front of System



Rear panels of SecureSync and Forward and Return (FRU) chassis

Note: the three blue lines are the interface cables (provided in the anc kit).

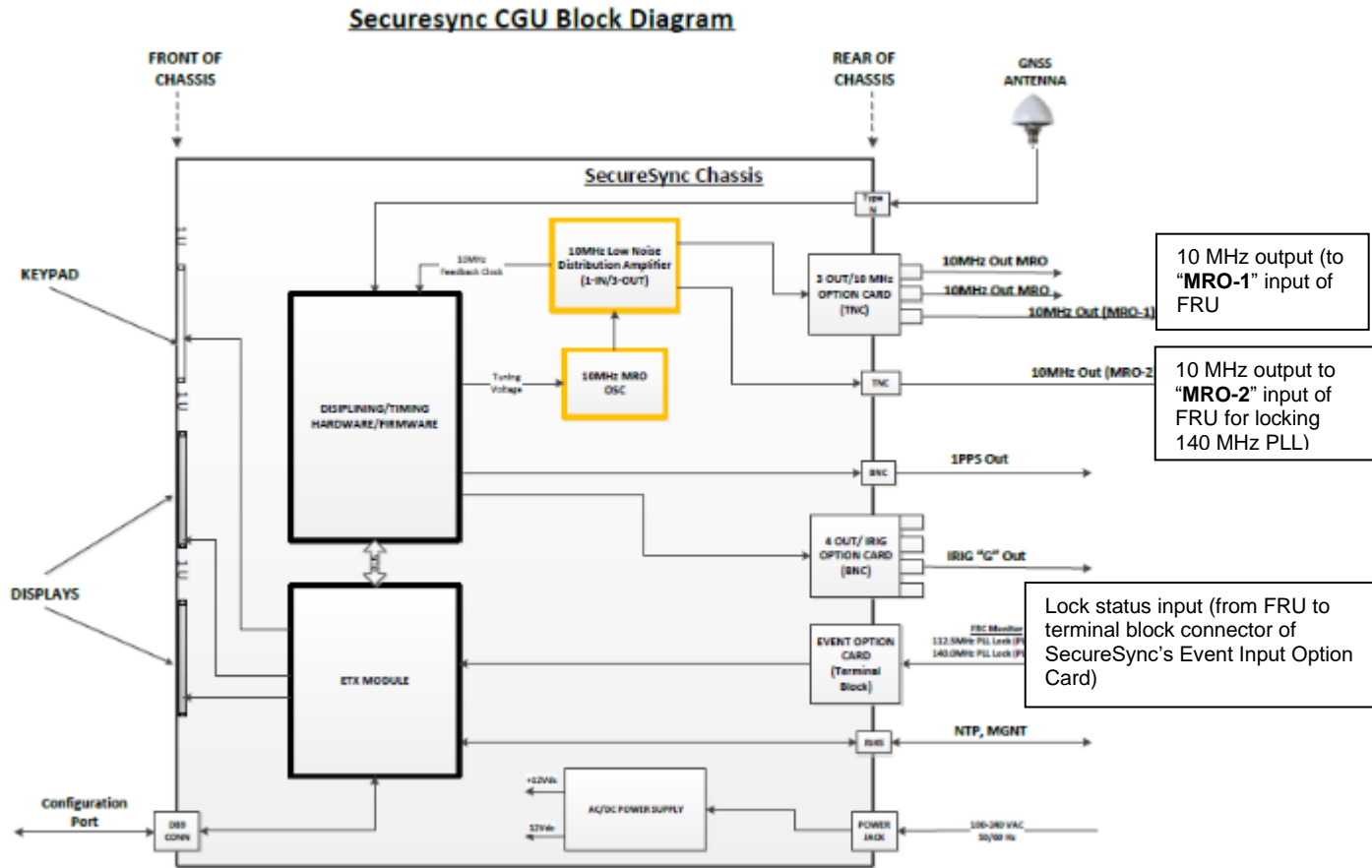


"PPR in" (input from a non-Spectracom device)

Figure 2 - Rear of System

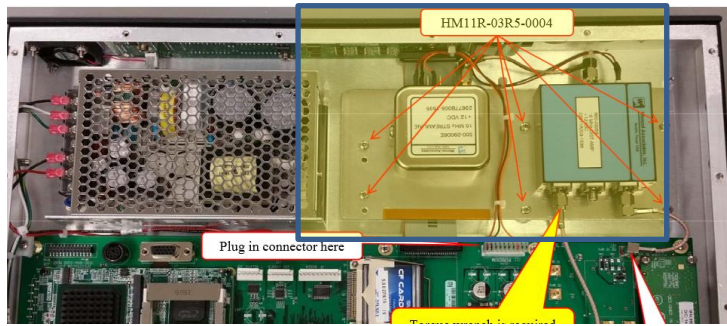
Two main Components:

1) SecureSync (1200-C001-0501)



**Hughes P/N: 150449-0011**

- This SecureSync is a modified (for very low phase noise) SecureSync C073,38,00,0D,00,15,00
  - 1204-15: (4) IRIG outputs
  - 1204-38: (3) 10 MHz outputs
  - 1204-0D: Event input card
- This SecureSync uses two internal components from Wenzel Associates (for very low 10 MHz output phase noise) as shown in upper-right corner of the photo further below.
  - **Note:** the Wenzel 10 MHz osc replaces the SecureSync's normal 10 MHz oscillator to become the primary/only 10 Mhz oscillator for the unit (its not a secondary oscillator receiving 10 MHz from another primary oscillator, like some other specials do). SecureSync discolplines the Wenzel osc and records its disciplining in the SecureSyncs's oscillator log (just like if it was our TCXO or OCXO)
    - **MP20R-0017-0001** (10 MHz amplifier): To bypass the standard onboard amps which would increase the phase noise)
    - **Y100R-0002-PC02** (10 MHz oscillator): this oscillator replaces (not in addition to) our oscillator with a very low phase noise osc that provides 10 MHz to the main PCB, the standard 10 MHz output connector and also to the (3)10 MHz output Option Card

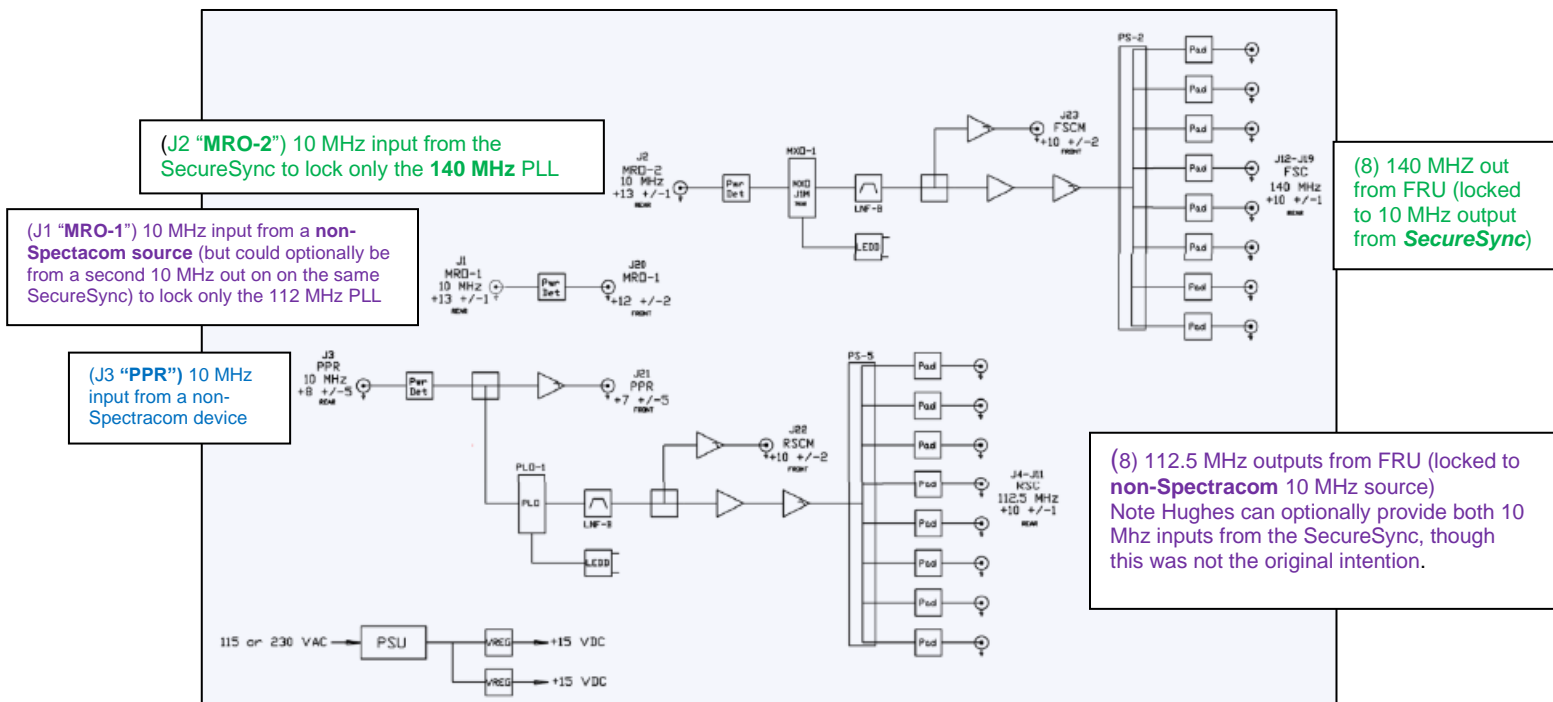


**Note-** There is no “onboard” 10 MHz TCXO/OCXO or a Rubidium osc installed in this SecureSync’s chassis. The Wentzel oscillator is the 10 MHz oscillator for the unit (the Wentzel oscillator is not a secondary 10 MHz osc in this particular special. It’s the primary oscillator for the SecureSync).

## 2) Forward and Return Clock Distribution chassis from Wenzel (referred to as: “CDC” / ”Clock Distribution Chassis” / “Wenzel Chassis”)

- **Our P/N:** MP41R-0002-0001 (in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1211945230&version\\_id=10370633288](https://app.bom.com/items/detail-spec?item_id=1211945230&version_id=10370633288))
- **Hughes P/N:** 150449-0011
- This is a custom device co-created by both Spectracom and Wenzel for Hughes.
- Front panel has status LEDs and PLL signal monitor outputs
- Rear panel has input power and input/output connectors
- No “smarts” in this unit. It’s just PLLS and LED indicators.

### Forward & Return Clock Distribution (FRU) Block diagram



### Interface cables we provide in anc kit

- Hughes SecureSync Anc Kit (1200-0000-0716) in Arena at: [https://app.bom.com/items/detail-bom?item\\_id=1214915411&version\\_id=10416069528](https://app.bom.com/items/detail-bom?item_id=1214915411&version_id=10416069528)
- **Hughes P/N:** 150449-0013 (for SecureSync) and 150449-0013 (CGU cables)

## ANC KIT, SECURESYNC HUGHES CGU CABLES

Revision: »2 - In Production | Effective as of 12/18/2015 10:57:34 AM, Unshared

Specs | **Bill of Materials** | Where Used | Sourcing | Costing | Files | Compliance | Revisions | Notifications | Supplier Access

Indented | Sourcing | Flat | Purchasing | Custom | Redline | Compare | Lookup

Contains 6 first-level Items, 10 line Items, 10 unique Items, 0 of which are shared.

| # | Item Number             | Item Name                                                    | Ca |
|---|-------------------------|--------------------------------------------------------------|----|
| 1 | 1200-1009-0801 rev 2 ρ  | SECURESYNC HUGHES CGU ANC KIT LABEL                          |    |
| 2 | CA01R-TNTN-0036 rev 1 ρ | CABLE ASSY,TNC MALE/TNC MALE, 36", DOUBLE SHIELDED RG58 COAX | ↑  |
| 3 | CA05R-D910-0001 rev 2 ρ | CABLE ASSY, HUGHES CGU STATUS CABLE, 36"                     | ↑  |
| 4 | MP02-0003-0002 rev 1 ρ  | LABEL STOCK                                                  |    |
| 5 | TM01R-0050-0001 rev 1 ρ | TERMINATION, SMA, MALE, 50 OHM, DC to 18000 MHz, 1.0 W       | El |
| 6 | TM03R-0050-0001 rev 1 ρ | TERMINATION, TNC, MALE, 50 OHM, DC - 11 GHz, 1.0 W           | El |

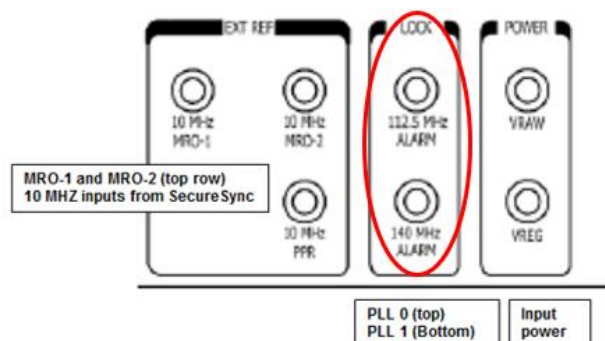
### Forward and Return unit's (FRU) PLL lock status (PLL Lock 0 signal and PLL Lock 1 signal)/Frequency Error alarm

- Refer to the CGU manual addendum for Hughes (1200-5000-C050) in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1217182411&version\\_id=10446313248&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1217182411&version_id=10446313248&orb_msg_single_search_p=1)
- There are two PLLs in the Wenzel Forward and Return Distribution Chassis:
  - **PLL Lock 0** for 112.5 MHz (which is locked to a **non-Spectracom** 10 MHz source, via the "PPR" input on the FRU)
  - **PLL Lock 1** for 140.0 MHz (which is locked to **SecureSync's** 10 MHz output, via the "MRO-2" input on the FRU)
- A problem with either PLL is fed back from the "FRU", into the SecureSync (via its Event input option card) and will result in a **Frequency Error alarm** being asserted in the Alarms log (alarms.log) and associated entries asserted in the oscillator log (osc.log)

### PLL Lock status indications available:

- LEDs on the front of the Wenzel clock distribution chassis (refer to "1" further below)
- In the SecureSync's browser (left side of the **Management** -> **Disciplining** page) (refer to "2" further below)
  - In the SecureSync's **oscillator log** (osc.log) (refer to "3" further below)

#### 1. PLL Lock Status LEDs the front panel of the Forward and Return chassis



#### 2. In the SecureSync's web browser

- Lock status for the two PLL circuits is reported on the left side of the **Management** -> **Disciplining** page of the browser (and are logged in the Oscillator log- refer to the info further below)

## 112.5 MHz and 140.0 MHz Lock Detect Indicators

The event option card was added to the SecureSync along with an adaptor cable that can be connected to the FRC. The 112.5 MHz and 140.0 MHz Lock Detect indicators are transmitted from the FRC chassis to the SecureSync for incorporation into the frequency alarm monitoring built into the SecureSync.

Indicators were added to the **MANAGEMENT > Disciplining** drop-down menu showing the status of the 112.5 MHz and 140.0 MHz lock detect.

The status indicators are as follows:

- **PLL-0 LOCK** = 112.5 MHz Lock Detect (Green = Locked, Red = Unlocked)
- **PLL-1 LOCK** = 140.0 MHz Lock Detect

### 3. SecureSync log entries associated with PLL lock status

Oscillator log (osc.log) entries associated with the two PLL lock statuses in the

```
[system] PLL_0 Lock Error (KAD)
[system] PLL_0 Lock Good (KAD)
[system] PLL_1 Lock Error (KAD)
[system] PLL_1 Lock Good (KAD)
```

#### Example entries in osc.log

|    |                 |          |                        |
|----|-----------------|----------|------------------------|
| 91 | Nov 03 00:31:48 | [system] | PLL_1 Lock Error (KAD) |
| 90 | Nov 03 00:31:48 | [system] | PLL_0 Lock Error (KAD) |
| 89 | Nov 03 00:31:30 | [system] | PLL_0 Lock Good (KAD)  |
| 88 | Nov 03 00:30:47 | [system] | PLL_1 Lock Good (KAD)  |
| 85 | Nov 03 00:13:39 | [system] | PLL_1 Lock Error (KAD) |
| 84 | Nov 03 00:09:10 | [system] | PLL_0 Lock Error (KAD) |

#### Log entries with a Frequency Alarm being asserted (problem unit)

Notice there aren't any Lock Good entries for PLL 0 (just PLL 1). So there appears to be an issue with PLL 0 causing the frequency Error alarm to be asserted

```
Mar 21 16:22:53 Spectracom Spectracom: [system] PLL_0 Lock Good (KAD)
Mar 21 16:23:41 Spectracom Spectracom: [system] PLL_0 Lock Error (KAD)
Mar 29 14:20:45 Spectracom Spectracom: [system] PLL_1 Lock Good (KAD)
```

**Log entries without Frequency Alarm being asserted) (good unit)**

Mar 29 14:04:49 Spectracom Spectracom: [system] PLL\_0 Lock Good (KAD)

Mar 29 14:05:27 Spectracom Spectracom: [system] PLL\_1 Lock Good (KAD)

**(Non-Wentzel oscillator SecureSyncs) Note PLL\_0 Lock Error (KAD) / PLL\_1 Lock Error (KAD) entries have also been observed on non-wentzel oscillator configuration.**

- In at least case (case **262649**) it appears it can happen if the KTS version isn't the correct version for the CFcard version installed (such as replacing the CF Card without then applying a software update)
- Based on a few other cases (203789 for instance) it appears these entries can simply be another indication the Rb oscillator is failing/has failed (not meaning anything different).

**Troubleshooting the “CGU system” (SecureSync and Wenzel chassis device – the FRU)**

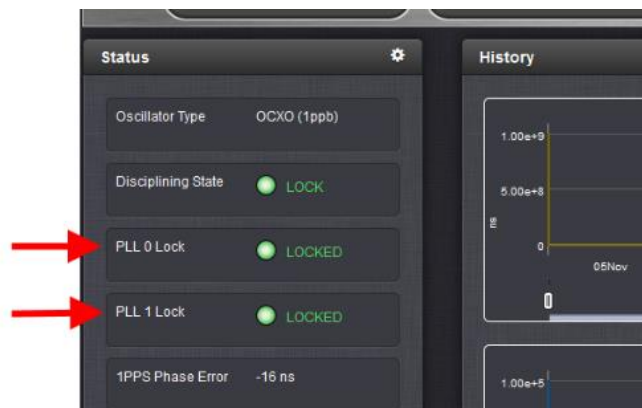
**1. Frequency Error alarm and “PLL\_0 Lock Error” / “PLL\_1 Lock Error” asserted**

**Note:** PLL Lock status/errors are sent from the FRU to the SecureSync’s Event Input Option Card to assert the Frequency Error alarm in the SecureSync

**Determine if the lock errors is associated with “PLL 0” (112.5 MHz) and/or “PLL 1” (140 MHz):**

- A) If the lock errors are with “PLL 0” only: PLL lock issue is associated with 10 MHz from the non-Spectracom 10 MHz source (or with the FRU)
- B) If the lock errors are with “PLL 1” only: PLL lock issue is associated with 10 MHz from the SecureSync (or with the FRU)
- C) If the lock errors are with both PLL 0” AND PLL 1” , the loc issue is not associated with 10 MHz output from the SecureSync. It has to be associated with the FRU itself (since the SecureSync only provides 10 MHz to lock the 140MHz PLL only. 10 MHz for the 112.5 MHz PLL is supplied to the FRU from a non-Spectracom source).

- 1) Look at the LED Lock indicators on the front panel of the Wenzel chassis (FRU)
- 2) Look at the two PLL lock status indicators (0 and 1) on the left side of SecureSync’s *Management -> Disciplining* page of browser:



- 3) Search the SecureSync’s osc.log for PLL Lock status messages.

- 4) Verify the interface cabling between the back of the SecureSync and the back of the Wenzel Chassis are “securely fastened.

## 2. “PPR input” Status LED on the front of the Wenzel chassis not lit

- “PPR” input is 10 MHz supplied from a non-Spectracom device to lock the 112.5 MHz PLL. Check to make sure this device is also connected to the Wenzel chassis.

### **Note about the oscillator log (osc.log) in this Hughes SecureSync special:**

As the **Wenzel** oscillator is the primary/only 10 MHz oscillator in this special SecureSync, the oscillator log entries in the unit, reflect the SecureSync’s software disciplining of the Wenzel oscillator itself. If there are any issues observed in the oscillator log (frequency or DAC jumps for instance), its associated with the Wenzel oscillator (not associated with another oscillator in the same unit, which is sometimes the case in other Specials using the Wenzel osc).

---

---

## B) PR4G Special

- Refer to ECO 1482 and 1527 (in Arena: [https://app.bom.com/changes/detail-affected?change\\_id=2392475342](https://app.bom.com/changes/detail-affected?change_id=2392475342))
  - Uses a SecureSync 1200-9030-0601 as the base, and adds an interal serial cable, and a 1204-48 Option Card
    - (SecureSync 223,02,1C,0F,48,11,00)
    - 1204-48 is a “PR4G Serial Port special”
- 
-

## Option Cards

**Schematics for the Option Cards:** (Refer to the 1204-xxxx) [\\rocfnp01\drivedata\Engineering\Archive\New Released\PCB Documentation](#)

For information all of the SecureSync Option cards, refer to

- [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards](#)
- Sharepoint site: [https://oroliagroup-portal1.sharepoint.com/Spectracom/customer\\_service/Shared%20Documents/Forms/AllItems.aspx](https://oroliagroup-portal1.sharepoint.com/Spectracom/customer_service/Shared%20Documents/Forms/AllItems.aspx)

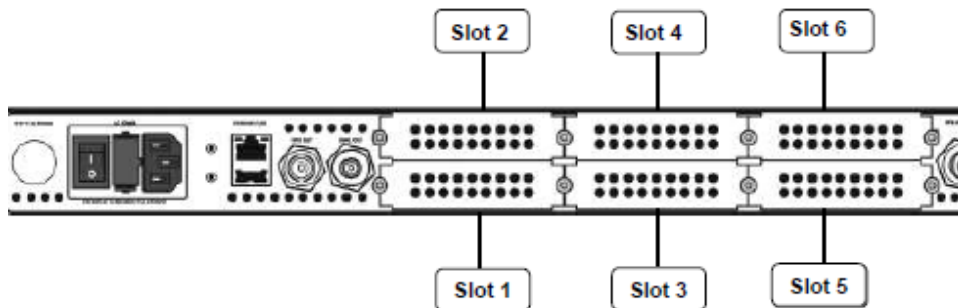
## API calls for Option Cards/Slots

- Refer to Tim Tetreault's "cheat sheet" at: [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\TSync driver calls cheat sheet](#)
- These are examples - additional calls may have since been added

| Option Card commands    |
|-------------------------|
| <b>DCS_GetCardInfo</b>  |
| <b>DCS_GetFeatByIdx</b> |
| <b>DCS_GetInstance</b>  |
| <b>DCS_GetOptions</b>   |
| <b>DCS_GetSlot</b>      |

## \*\*Slot Numbers

The six option module card bay slots are designated as Slot 1 – Slot 6, as shown in the following figure:



*SecureSync Rear Panel Option Module Bays*



### Ribbon cable for top row

- When we send new Option Cards to be installed in the field, a kit that includes a 50 pin ribbon cable (ribbon cable is our P/N CA20R-R200-0R21) and the Install guide mentioned above, is provided with each card. This ribbon cable provided is only used when installing an Option card in the top row (Bays 2, 4 and 6). The ribbon cable is not used with the bottom row of Option Cards (Bays 1, 3 and 5).

#### Ribbon cable should be “looped outward”

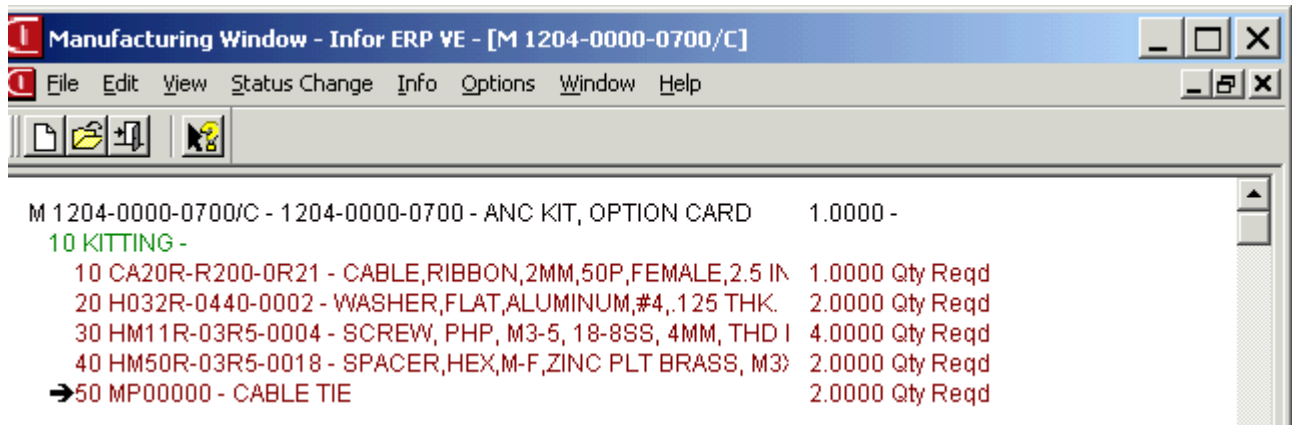


#### Don't install the cable “looped inward”



### Ancillary kit included with Option Card purchases

- The P/N for the ancillary kit is 1204-0000-0700. This ancillary kit includes:



- If a customer desires to move a card that is installed when the SecureSync was purchased, from the bottom row to the top row, they will need the kit above (which includes the ribbon cable to connect the Option Card to the main board).

---

## System Memory (SecureSync and Option Cards) / Sanitization/

### \*\*GPS receiver memory and CF Card/System memory in SecureSync

Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Memory\SecureSync memory.pdf>

**Note:** Manufacturer's names and P/Ns subject to change. Do not release to customers, though memory sizes can be released as appropriate.

**Note:** This document has an FAQ that refers to the “/dev/hda1” file. This is the name of the mounted installed CF card in its entirety. So the FAQ is referring to all files on the CF card itself.

Q. What is the capacity of the Main Memory? (Ex.: 256 MB)

A. **SecureSync has 512MB of RAM and a 1GB Compact Flash card.**

---

### \*\*Certificate of Volatility (COV)/ Letter of Volatility (LOV)

- In online SecureSync user guide at:  
[http://manuals.spectracom.com/Other/SecureSync\\_OptionCards\\_CertOfVolatility.pdf](http://manuals.spectracom.com/Other/SecureSync_OptionCards_CertOfVolatility.pdf)
- “**COV-SecureSync**” in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1277512546&version\\_id=11522546318](https://app.bom.com/items/detail-spec?item_id=1277512546&version_id=11522546318)
- “**COV-OptionCards**” in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1277512573&version\\_id=11522546778](https://app.bom.com/items/detail-spec?item_id=1277512573&version_id=11522546778)
- Refer also to <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Memory>

---

### Procedure to sanitize the CF card

- 1) Upload the same as already installed, or newer, Archive version of software via FTP/SCP (such as load 5.1.2, if 5.1.2 is already installed).
- 2) Perform a “**Clean Upgrade**” command via the CLI interface.

**Clean upgrade** (Such as first performing a Forced upgrade from 4.8.8 to 4.8.9, for example. Then automatically resetting the NTP server back to factory default settings and deleting all log files): “**sysupgrade clean**” followed by the upgrade file name (Example: **sysupgrade clean update489.tar.gz**).

### Software issue after performing clean upgrade (with 5.8.2 and below installed) affecting TACACS logs

**Symptom: Can access SSH via TACACS, but not the browser (applicable to versions 5.8.2 and below)**

- **Per the v5.8.3 (Jan 2019) Release Notes** “Fixed an issue in which **clean updates** wouldn't allow TACACS+ access through http”

---

### Desire for a customer to send us blank CF cards to program for them

- We can do this for a customer, but they must be ones that we have tested/verified compatible with SecureSync
- Make sure customer is aware that the CF cards can be wiped/CF card sanitized. Send the SecureSync memory document.
- BAE systems is sending us like 5 of the following blank CF cards to try to burn for them (refer to salesforce case 15596). These appear to work just fine in the system.

- WD SiliconDrive II
- 1 GB PATA
- SSD-C01GI-4600

**Email to Tim Carter with BAE systems (21 Aug 2014) (Salesforce case 15596)** To begin, attached you should find the document I alluded to that discusses how to sanitize the SecureSync (including how to completely clean the CF card of everything except the OS and factory default settings).

As for burning a batch of CF cards that you supply is with, we can do this for you as long as they are a brand/Model that we have tested and confirmed are compatible with the SecureSync. Please note that not all CF cards are compatible with this product. We ran into issues early on when trying to use standard-off-the-shelf CF cards programmed with our software. The ones we now use are an industrial grade CF card.

If you don't already have cards that we have confirmed as compatible, let me know and I will send you like four additional cards that you can use. Just keep in mind the cards can be wiped using the document I have attached. The brand/item number for the CF cards we recommend and currently use are from Smart Technologies and heir P/N is SG9CF1GHYB4AX.

If you would like to send us a batch of these particular CF cards, we will be happy to program them for you. Otherwise, let me know and I will send you a few of ours, already programmed.

---

### **Cost to replace a CF card (due to security concerns)**

- \$50.00 each plus 25.00 shipping

**Email Keith sent to the USAF** Keep in mind that there is a method available to wipe the CF card without having to replace it. But if you prefer to replace it with a new one that has been pre-programmed, they can be purchased from us, as desired.

---

## \*\*ETX Microprocessor memory

[http://www.advantech.com/products/SOM-4455/mod\\_37BFA971-A650-4458-9588-F569B005CF78.aspx](http://www.advantech.com/products/SOM-4455/mod_37BFA971-A650-4458-9588-F569B005CF78.aspx).

**Data sheet (tech info):** [http://download.advantech.com/ProductFile/PIS/SOM-4455/Product%20-%20Datasheet/SOM-4455\\_DS%2806.13.12%2920120622152856.pdf](http://download.advantech.com/ProductFile/PIS/SOM-4455/Product%20-%20Datasheet/SOM-4455_DS%2806.13.12%2920120622152856.pdf)

**ETX RAM:** 512 MB RAM

**ETX BIOS memory:** Award 4Mbit (512kb) Flash BIOS

---

### Timing System memory (on main board)

8KB EEPROM

Size of memory: 8KB (64 kbit)

Type of memory: EEPROM

MFG: Atmel

**Mfg P/N:** AT25640

8MB Flash

Size of memory: 8MB (64 Mbit)

Type of memory: SDRAM

**MFG:** Micron Technology

**Mfg P/N:** 28F640J3D75A, 28F640J3F75A

RAM memory

**Size of RAM:** 8MB (64 Mbit) SDRAM

Type of RAM: SRDAM

**MFG:** Micron Technology

**Mfg P/N:** MT48LC4M16A2

ColdFire MCF5216 microcontroller

(contains 512kb Flash and 32kb SRAM (Volatile Scratch RAM))

**Size/Type of Memory:** 512kb Flash (ColdFire V2CORE) and 32kb SRAM (Scratch volatile memory)

**MFG:** Freescale

**Mfg P/N:** MCF5216

**Note:** the ColdFire MCF5216 microcontroller is not part of the ETX processor. It's another processor on the main board itself, completely separate from the ETX module.

Option Cards with NVRAM IC have an 8MB IC

**Size of memory:** 8Mbit (not 8MByte)

**MFG:** Adesto

**MFG P/N:** AT25DF081A

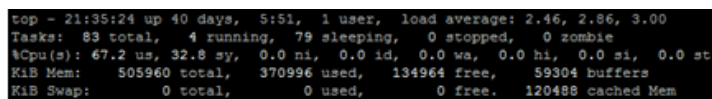
**Link to manufacturer website** (<http://www.adestotech.com/sites/default/files/datasheets/doc8715.pdf>)

**Type of 8Mbit RAM:** Serial interface Flash (non-volatile memory)

---

### Report of swap memory usage

- May be monitored by solar winds (solarwinds) for example.
- Swap is reported at the beginning of the non-spectracom specific “**top**” cli command.
- Swap is reported as “0 total”, since there is no swap memory in the system:



```
top - 21:35:24 up 40 days, 5:51, 1 user, load average: 2.46, 2.86, 3.00
Tasks: 83 total, 4 running, 79 sleeping, 0 stopped, 0 zombie
%Cpu(s): 67.2 us, 32.8 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 505960 total, 370996 used, 134964 free, 59304 buffers
KiB Swap: 0 total, 0 used, 0 free, 120488 cached Mem
```

Q. (from George Siaw with Hughes) SNMP monitor of the spectracom GPS keeps telling us this. (Swap Memory has exceeded threshold: (60%) currently (100%))

A (from Dave Sohn) This should be ignored. There isn't any swap memory to exceed, or be below, a threshold.

## Sanitization

- Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Memory\SecureSync memory.pdf

### Email from Denis Reilly:

Customers can apply upgrades, provided by us, that upgrade the functional logic of the FPGA. Customers can't put arbitrary data in the Option Card FPGA EEPROM, and no user data ever goes into the FPGA EEPROM: the only data the customer puts there is data that we provide. (either the initial image that ships with the unit, or any other data we provide as part of the upgrade process.)

The only exception is the PTP card, as I have described.

Applying a forced upgrade to the unit will ensure that the option card FPGA images get reverted to a known state, which may be what the customer is going for.

## Model and Serial Number

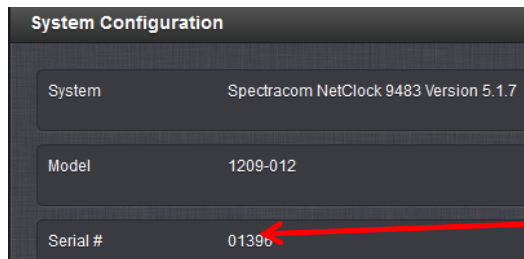
- CLI command to get the Model and Serial number: **model** <enter> (Note: this command is not available in all earlier versions of software- Not sure at what version of software this comamd was eventually added)
- Per Denis Reilly, the unit's Serial Number is stored in the EEPROM on the main logic board.

### Obtaining Model and Serial Number remotely

#### A) Via web browser

##### 1. Newer black web browser:

Tools -> Upgrade/Backup page of the browser (under "System Configuration")



##### 2. Classic interface browser

**Note:** Post version 4.4.0 updates should have the Model/Serial Number at the top of the **Tools -> Versions** page.

Note that the reported "Archive Version" is the "common reference" for all of the various software versions installed in the SecureSync. The "Archive version" defines all of the different versions of software installed. When a software update is applied to any of the various software modules, the "Archive Version" is updated, as well.

#### B) Via CLI (telnet, ssh or serial connection)

- Use the CLI command of **model** <enter> (lower-case)
  - **Note:** this command is not available in all much earlier versions of software- Not sure at what version of software this command was eventually added)

```
spadmin@Custservice /home/spectracom/mibs $ model
NetClock 9483
Model No: 1209-012
Serial No: 01396
spadmin@Custservice /home/spectracom/mibs $
```

**Note:** Can also use the command: **LS\_GetSerialNo 0**

```
spadmin@Spectracom ~ $ LS_GetSerialNo 0
Serial Number: 01396
Model Number: 1209-012
spadmin@Spectracom ~ $
```

### C) Model/Serial Number Via SNMP

- Serial Number via SNMP was added in version 5.2.1 software update.
  - The Model and Serial Number are not available via SNMP in version 5.2.1 and below, refer to Mantis Case 1855).

Q. Is the Serial Number and Hardware Version available via SNMP? If so, what OIDs should we use? We've looked through the provided MIBS, but didn't find anything.

A. At this time, the Serial Number and Hardware Version information are not available via SNMP. The unit's Serial Number can be found on the Serial Number tag affixed to the appliance. We do not provide any "Hardware version" information. However, the "Software versions" for the various SecureSync modules can be obtained from the Tools/Versions page of its web browser.

### D) Model/Serial Number via the logs

- Version 5.2.1 update (Apr 2015) added Model and Serial Number to the **System Log** at each start-up.

---

## Reprogramming Model Number (Power/Oscillator/Receiver) or Serial Number

- The programmed Model Number (Part Number) affects the software power configuration. A missing or incorrect Part Number will result in the unit thinking the input power configuration is different than the actual input power input configuring, resulting in an alarm being asserted.
- The unit's Serial Number (Tools ->Versions page) can be entered, if it was inadvertently not programmed or if it was programmed incorrectly when the SecureSync/NetClock was shipped.

### A) Reprogramming a missing or incorrect Model/Part Number (which can affect the AC/DC input power configuration, oscillator and receiver configuration)

- 1) telnet or ssh into the unit (can't change values via the web browser)
- 2) login as "spfactory".
- 3) type: **modno** <enter> Response will prompt for the desired unit's Model Number.
- 4) Enter the correct 14 digit Part Number and press <enter> (Note: this is the 12 digit P/N and counts the two dashes): **Example: 1200-0237-0601** <enter> (the example consists of 12 digits and two dashes)
- 5) Reboot/power cycle the unit for changes to take effect.

```
Spectracom login: spfactory
Password:
Spectracom NetClock 9483 Version 4.8.6
[spfactory@Spectracom ~]# modno
Enter Part Number:1209-012
Error: Invalid part number (1209-012)
Part numbers must be 14 characters.
[spfactory@Spectracom ~]# 1209-0002-0601
```

## B) Reprogramming a missing or incorrect unit's Serial Number

- 1) telnet or ssh into the unit.
- 2) login as "spfactory".
- 3) type: **serno** <enter> Response will prompt for the desired unit's Serial Number.
- 4) Enter correct Serial Number and press <enter>
- 5) Reboot/power cycle the unit for changes to take effect.

**Note:** After rebooting/power cycling to have the Model Number or Serial Number change take effect, the web browser may display "the web browser encountered an unexpected error...". Refer to Mantis case 1982.

```
Linux 2.6.15-USAGI <spectracom.int.orolia.com> <0>
Spectracom login: spfactory
Password:
Spectracom NetClock 9483 Version 4.8.6
[spfactory@Spectracom ~]# serno
Enter Serial Number:01397

Starting EEPROM upgrade process.

Image file:
Mark:      0xDEADBEEF
Type:      0x00000006
Length:    0x000000C4
Version:   1.00
CRC:       0x34903638

Sending... done

Upgrade status: 100% complete...

EEPROM upgrade process completed successfully.
Reset required to take effect.

[spfactory@Spectracom ~]# _
```



---

## **\*\*SecureSync calibration service**

- There is no calibration required/available for the SecureSync or its Option Cards
- The SecureSync is self-calibrated to an external input reference (such as GPS)

**Email Keith sent to Hongbo (16 Jan 2013)** Is this regarding a SecureSync that has already been purchased and shipped to your customer? Or is this regarding an order that the customer will be submitting to us sometime in the future?

I don't believe we have provided any customer yet with a Calibration Certificate for SecureSync. We can supply Certificates of Conformance for this unit, but note that there really isn't anything in SecureSync to actually "calibrate".

SecureSync is a self-calibrating device (when locked to GPS, IRIG, etc). The oscillator calibrates itself and there are no tunable items in the unit (no potentiometers or other adjustable components). Calibration service would really be limited to the same items included in the certificate of Conformance, which covers the tests normally performed during factory production. The calibration service would essentially entail verifying voltage measurements and also the normal operation of the unit, since there are really no adjustable items in the unit.

If your customer requires this calibration sticker, we will need to come up with a price for this service. Also, the SecureSync would need to be returned to us (if this is for a unit that has already been purchased from us and shipped to the customer, it would need to be returned for the first calibration and then every year thereafter, if they wished to renew the calibration certificate). All shipping fees and the established calibration service fee (the minimum cost for the calibration service fee will be at least \$200.00 USD as this is the minimum evaluation fee for all non-warranty returns).

If your customer still wants to have the unit re-tested as it was during the manufacturing process for a certificate, we will establish an actual cost for this service. But as there are no adjustable items in this unit, I would like to first verify your customer still wants this test performed, with this understanding.

Please let me know if this is for a new order that has not yet shipped to the customer, and if they still want this calibration service performed, with the understanding there really isn't anything to "adjust" in this particular unit, as it's designed to be self-calibrating. Then, we can go from there!

## Software version/Software update/Software downgrade/restore to defaults

Refer to: [\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates](#)

### General software release info

- Refer to **Excel spreadsheet** for info on all update releases: I: Cust Service/PSBs/
- Detailed Engineering Release Notes for each release : Search SAP-> Files for “[Jira\\_Export\\*](#)”

### “SW VVersion” (installed Version wasn’t reported in one particular update, and two Vs present)

```
System  
Spectracom  
NetClock  
SW VVersion
```

- From elsewhere in this same document: “I believe it was version 5.2.1 that had the issue with the version field in the browser being blank (null). But I’m not positive and not finding any references to it to confirm (either in this document or in Mantis)”

### Obtaining currently installed version information

- Update software version 5.2.0 enhanced the version info being reported in the Tools -> Upgrade/Backup page of the browser.
- Now reports versions of Apache, NTP, OpenSSL, NetSNMP, OpenSSH, PHP (for newer black/charcoal browser), KTS version, etc.

### Obtaining the currently installed Archive / Timing System software versions:

- Reported in the [Tools](#) -> [Versions](#) page of the web browser.
- Automatically reported when logging in with telnet/ssh (displayed after entering the correct password). Refer to: [Command line interface \(CLI\)](#) further down.

```
login as: spadmin  
Using keyboard-interactive authentication.  
Password:  
Spectracom NetClock 9483 Version 4.8.6  
[spadmin@Spectracom ~]$  
[spadmin@Spectracom ~]$ █
```

- Login via telnet/SSH and type “version” (Version command returns Archive and Timing System version) Refer to: [Command line interface \(CLI\)](#) further down.

```
[spadmin@Spectracom ~]$ version  
Software      4.8.6  
Timing System 2.8.6  
[spadmin@Spectracom ~]$ █
```

---

## Obtaining the versions of the installed software packages (such as Apache, GPS, SNMP, NTP, etc):

There are “**version**” commands available for the installed packages, via the CLI interface. Refer to: [Command line interface \(CLI\)](#) further down.

---

## \*\*Software Licenses/EULAs for the SecureSync’s internal firmware

- Refer to Salesforce cases such as 283715
- Customers/resellers periodically ask if there are any software licenses or a EULA associated with SecureSync’s internal firmware.
  - There are Software licenses available to use open-source packages within the firmware. Refer to (“License Notices” section) the online SecureSync user guide at: [https://orolia.com/manuals/SS/Content/NC\\_and\\_SS/Com/Topics/APPENDIX/LicenseNot.htm](https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/APPENDIX/LicenseNot.htm)
  - There is a EULA associated with Opt-IDM (BroadShield/JADE). As of at least 5.9.4 and below (April 2022) there is no “EULA” for the standard firmware installed in SecureSync:

*Excerpt from Case 283715:*

Q I'm looking for the end user license agreement for the SecureSync 1200 update package (version 5.9.4). I took a look through the release notes and upgrade guide, as well as the update package but couldn't find it. Maybe I'm just looking in the wrong spot?

A (from Keith April 2022) I am only aware of one End User license Agreement (EULA) for SecureSyncs. This EULA is specifically for just one optional software suite (Opt-IDM: Interference detection mitigation). Opt-IDM consists of one of two software options. Opt-BSH is for the full software suite, for both GNSS jamming and spoofing detection/mitigation. Opt-JADE is a partial of the same suite, consisting of just the GNSS jamming detection/mitigation portion (JADE doesn't provide the spoofing detection that Opt-BSH provides).

I believe what you are looking for are the permissions to use the various packages within the SecureSync's software (such as the open-source NTP package, for instance). This info is in the online Model 1200 SecureSync user guide. This available guide has the most up-to-date info on the device and is very easily searched. The direct link to this info (“**License Notices**” section) is the following: [https://orolia.com/manuals/SS/Content/NC\\_and\\_SS/Com/Topics/APPENDIX/LicenseNot.htm](https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/APPENDIX/LicenseNot.htm).

**(follow-up question)** Q Am I correct in my understanding then that as there's no EULA, we are free to do whatever we would like with the SecureSync 1200 firmware without restriction?

**RESPONSE FROM Emmanuel (21 April 2022)** SecureSync 1200 firmware is not sold separately from a SecureSync unit and is not licensed in any way. Therefore General Dynamics actually cannot do anything with the SecureSync firmware on its own. Other than this, General Dynamics can do whatever they want with the SecureSync unit (as long as meeting regulations), including reselling the full SecureSync unit with its installed firmware (making sure that export control rules are met).

---

## \*\*Performing software updates/Step Update requirements

- All versions of software support updating the software via the web browser.
- Starting in Archive version 4.8.8, software updates can be performed without the use of the browser, if desired (using the CLI interface). The upgrade bundle can be transferred in using FTP/SCP. Then, the upgrade can be started using Telnet or SSH commands. Refer to the software upgrade instructions for more information on using the CLI or the web browser to perform updates.

### Step-update requirements

- Refer to each version of the Update Release Notes for step-update requirements.
- Step updates are needed to prevent the loss of configs when updating from earlier versions to a newer version

#### Step update to version 5.8.2

(As also mentioned in the next section below) Version 5.8.2 is a necessary step-update file The original release/cut-in of 5.8.2 (ECO-FAI-1876, 10/19/2018) contained FSMLabs Timekeeper functionality. As this had to be removed for legal reasons, version 5.8.2 (version info remained the same) was re-released on ECO-2566 9/9/2020. The original 5.8.2 update files were removed from SAP.

Refer to [ECO-2566](#) folder to obtain version 5.8.2 to send to customers.

---

## Specific software version notes (info not necessarily in release notes)

- Version 4.5.1 is going to be to allow more than 12 IRIG outputs out of SecureSync. 12 is the current limit on the number of digital pots. A customer wants more than 12 IRIG outputs so this will be a deviation.
- Version 4.6.0 will be to release Model 9483 and fix Ethernet routing tables. It may also incorporate the STOB (Stanag Option Card).
- Version 5.2.1: I believe it was version 5.2.1 that had the issue with the version field in the browser being blank (null). But I'm not positive and not finding any references to it to confirm (either in this document or in Mantis)
- Version 5.4A? (Harris only- replacement to v5.2.D) Software change associated with GPS 1PPS steering of the oscillator due to the GPS Timing error condition affecting their systems. Refer to the Oscillator Disciplining section for details of this change (search for "5.4A")
- Version 5.8.2: The original release/cut-in of 5.8.2 (ECO-FAI-1876, 10/19/2018) contained FSMLabs Timekeeper functionality. As this had to be removed for legal reasons, version 5.8.2 (version info remained the same) was re-released on ECO-2566 9/9/2020. The original 5.8.2 files were removed from SAP.

Refer to [ECO-2566](#) folder to obtain version 5.8.2 to send to customers.

---

## Update log/entries

- Update log is not displayed in browser, but captured in the standard log bundle.
- Update log can be viewed via CLI (logs directory).
- Updates that are performed are reported in the Tools -> Versions page of the web browser.
- Logs record when the update was performed, version it was updated to, etc.
- If "Restore Factory Configuration" update was also selected (or if the clean command was used when performing the update a via a CLI command) when the update was performed, all logs (and configs) are cleared. There will be no Update log entries after the update is performed.

---

## Cleaner File/Software updates/upgrade issues

### Cleaner file

- P/N: 1200-SU02-CLNR
- In Arena: [https://app.bom.com/items/detail-spec?item\\_id=1208963719&version\\_id=10692855408&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1208963719&version_id=10692855408&orb_msg_single_search_p=1)
- On our website: <https://files.spectracom.com/public-downloads/latest-securesync-netclock-files>
  - Link is at the bottom of the first paragraph

### how to tell when cleaner has completed

| PACKAGE     | Old Version | New Version | ACTION               | STATUS    |
|-------------|-------------|-------------|----------------------|-----------|
| Application | 5.4.1       | -           | No Upgrade Available | Completed |
| Timing FW   | 3.31        | -           | No Upgrade Available | Completed |
| Timing FPGA | 3.31        | -           | No Upgrade Available | Completed |
| OC 1 ID 1E  | 0101        | -           | No Upgrade Available | Completed |
| OC 2 ID 1E  | 0102        | -           | No Upgrade Available | Completed |
| OC 3 ID 1E  | 0102        | -           | No Upgrade Available | Completed |
| OC 4 ID 1E  | 0102        | -           | No Upgrade Available | Completed |
| OC 5 ID 1E  | 0102        | -           | No Upgrade Available | Completed |
| OC 6 ID 1E  | 0102        | -           | No Upgrade Available | Completed |
| Licensing   | -           | -           | No Upgrade Available | Completed |
| GR02        | 0000        | -           | No Upgrade Available | Completed |
| HotPatch    | 5.4.1       | XXXX        | No Upgrade Available | Completed |

FYI- The “**Upgrade Failure**” in red at the top is because the cleaner doesn’t change the installed software version (such as version 5.4.1 in this instance). This report is expected every time the cleaner is performed.

The primary indication the cleaner has completed successfully is the last row of the “Upgrade Status” window (labeled “Hot Patch”) reporting “Completed” (in green) All of the other rows will indicate “no upgrade available” and “completed”. The only row which matters for the cleaner is this last row. It will also indicate “no upgrade available” (because it doesn’t change any version numbers). When this last row reports “Complete” the cleaner is all set!

It’s ready for version 5.7.0 to be applied (very similar process, just different file/filename selected in the dropdown).

- Upgrade bundles are uploaded into the home/spectracom directory

### Typical Update log (example for 5.4.5 to 5.4.6)

```

Sep 13 13:37:40 Spectracom Spectracom: [sw-upgrade] Using update tool supplied by upgrade (SWUAL)
Sep 13 13:38:56 Spectracom Spectracom: [spupdate] Application 5.4.5 5.4.6 Upgrade Needed (SWUE)
Sep 13 13:38:56 Spectracom Spectracom: [spupdate] Licensing - No Upgrade Available (SWUE)
Sep 13 13:38:56 Spectracom Spectracom: [spupdate] Licensing - No Upgrade Available (SWUE)
Sep 13 13:38:56 Spectracom Spectracom: [spupdate] Timing FW 3.36 3.36 No Upgrade Needed (Will Force) (SWUE)
Sep 13 13:38:57 Spectracom Spectracom: [spupdate] Timing FPGA 3.36 3.36 No Upgrade Needed (Will Force) (SWUE)
Sep 13 13:38:57 Spectracom Spectracom: [spupdate] GNSS 0000 1.9 No Upgrade Available (SWUE)
Sep 13 13:38:57 Spectracom Spectracom: [spupdate] Timing EEPROM 1.00 No Upgrade Available (SWUE)
Sep 13 13:38:57 Spectracom Spectracom: [spupdate] OC 1 ID 1F 0102 1.02 No Upgrade Needed (Will Force) (SWUE)
Sep 13 13:38:57 Spectracom Spectracom: [spupdate] OC 2 ID 06 0000 - No Upgrade Available (SWUE)
Sep 13 13:38:58 Spectracom Spectracom: [spupdate] OC 3 ID FF 0000 - No Upgrade Available (SWUE)
Sep 13 13:38:58 Spectracom Spectracom: [spupdate] OC 4 ID FF 0000 - No Upgrade Available (SWUE)
Sep 13 13:38:58 Spectracom Spectracom: [spupdate] OC 5 ID 01 0103 1.03 No Upgrade Needed (Will Force) (SWUE)
Sep 13 13:38:59 Spectracom Spectracom: [spupdate] OC 6 ID 32 0127 1.27 No Upgrade Needed (Will Force) (SWUE)
Sep 13 13:38:59 Spectracom Spectracom: [spupdate] Upgrading Option Card 1f Run-Time in Slot 1 (SWUE)
Sep 13 13:39:39 Spectracom Spectracom: [spupdate] Upgrading Option Card 1 Run-Time in Slot 5 (SWUE)
Sep 13 13:40:25 Spectracom Spectracom: [spupdate] Upgrading Option Card 32 Run-Time in Slot 6 (SWUE)
Sep 13 13:56:21 Spectracom Spectracom: [spupdate] Upgrading KTS Firmware (SWUE)
Sep 13 13:57:19 Spectracom Spectracom: [spupdate] Preparing Application Software for Upgrade (SWUE)
Sep 13 14:11:25 Spectracom Spectracom: [sw-upgrade] Upgrade Initiated, Reboot Required:
/home/spectracom/update546.tar.gz (SWUAL)
Sep 13 14:23:28 1 1: [TRANSFER_ENGINE] Update successful

```

### Software Upgrade issues

- If there are issues with the software update of the SecureSync, or any installed Option Cards, request all of the log entries in both the “**Update**” and “**System**” logs for our review. The two sets of logs will likely indicate why an update failed.

#### 1. actual (truncated) Update.log entries for an upgrade failure

```

[sw-upgrade] Using update tool supplied by upgrade (SWUAL)
[sw-upgrade] Using update tool supplied by upgrade (SWUAL)

```

## 2. actual (truncated) System.log entries for an upgrade failure

```
[spupdate] Starting Update (SWUE)
[WEB] Log SQLSTATE[HY000]: General error: 13 database or disk is full (WEB)
[spupdate] ERROR (-1) - Problem unpacking Update Bundle. (Is the file corrupted?) (SWUE)
[spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)
[sw-upgrade] SW Upgrade Error (8) (SWUE)
[spupdate] Starting Update (SWUE)
[WEB] Log SQLSTATE[HY000]: General error: 13 database or disk is full (WEB)
[spupdate] ERROR (-1) - Problem unpacking Update Bundle. (Is the file corrupted?) (SWUE)
[spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)
[sw-upgrade] SW Upgrade Error (8) (SWUE)
```

### SecureSync update process:

#### A) Potential loss of configurations: The Config file “Transfer engine” has a “20 version update step” limit

- Refer to Salesforce Cases such as 178239
- Applicable to at least software versions 5.8.2 and below (not certain if/when a change will be incorporated, but likely it will be in 5.8.3 or 5.8.4 if a change is possible)
- Applicable to both the software update process and to config file restores.
- Loss of configurations can occur if there are **more than a total of 20 software updates** (both updates released to production as well as all Engineering releases not released to production- such as versions 5.4.A and 5.7A for examples) between the start version (such as v5.0.2 for instance) and the version the configs are being restored to (such as 5.8.2)

#### *Two emails from Stuart to Dave L (13 Nov 2018)*

##### Concerning updates from 5.0.2 to 5.8.2:

It is known that you cannot transfer configurations from 5.0.2 to 5.8.2. SecureSync's transfer engine can only handle ~20 version transfers in one upgrade. It is not clear at this time what will happen to their configurations if they exceed this ~20 upgrade path maximum (it appears to stop after 20 versions and declare the transfer as “successful”).

Starting at version 5.0.2, they can maximally transfer configs to version 5.2.0, from 5.2.0 to 5.4.3, from 5.4.3 to 5.7.1, and from 5.7.1 to 5.8.? (TBD, but at least 5.8.3).

- I have just tested this and can confirm that the transfer engine will drop all configuration transformations past 20 transfers.

This means configurations at an older version may not be properly updated to reflect any necessary changes that should take place between an older and newer version of SecureSync.

Below is the easiest path a customer can traverse to 5.8.2 while safely maintaining their configurations.

- The earliest version which can reach 5.8.2 is 5.5.0
- The earliest version which can reach 5.5.0 is 5.1.1
- The earliest version which can reach 5.1.1. is 5.0.2

*Once again bear in mind that this is also true for config bundles. This issue will be remedied in 5.8.3.*

**Email Keith sent to Eric Girard (13 Nov 2018)** I wanted to make sure you are aware of something that the rest of us JUST learned, pertaining to SecureSync/9400 configs. When either performing software updates, or when installing an earlier version configuration backup bundle to a newer installed version, there is (at least currently) a “20 version step” limit of the configs actually being restored.

The “version steps” in between the version the configs are being restored from (such as upgrading from version 5.0.2, or restoring a config bundle which was saved at version 5.0.2 to a unit now running 5.8.2) includes all full releases, and all engineering only releases (such as version 5.4.A for instance) from that point forward to the newly installed version. If there are more than 20 total software versions between the starting version and the newer version, the config transfer engine won't restore the configs to the newer version.

But if a “step” / interim software update is first performed (which is no more than 20 versions away from the starting/current version) before updating to the latest version of software, the configs will transfer to the “step” interim version. An example of this

step is to update v5.0.2 to 5.4.0 first and not just update it directly to 5.8.2.

If there are only 20 versions between the one step/interim version and the final desired version, it can then be updated from the one step to the latest version with all configs being retained. With a very early starting version (such as v5.0.2 for example) a total of like three or four software updates to interim versions is required, if its desired to retain configs being restored during an update to version 5.8.2 (as Dave Lorah just had reported to him from a customer ☹️)!!!!!!

If a customer updates a SecureSync/9400 directly from v5.0.2 to 5.8.2 for instance, v5.8.2 will still be applied OK. But because there are many more than 20 versions in between, the current settings/configs will be lost when it has been upgraded to 5.8.2 (the customer will need to manually restore their desired configs)

Engineering will be looking into changing/removing this "20 step" limit on the transfer engine. But this won't be incorporated until update version 5.8.3 at the earliest. So, this 20 step limit will be in place until the change has been added into a newer version.

The biggest potential condition is if a customer is updating a remotely installed unit, from an earlier version. Then during a software update process, they then lose the settings which allow them to access it remotely.

I have asked that Dave Sohn add a notice on the same web page where customers download the software update bundles, that advises our customers that they may potentially lose configurations when applying a software update, especially when there have been no software updates applied in a very long time.

---

## B) Updating to v5.6.0 or above with at least three 1204-12 10/100 PTP cards installed causes upgrade failure

- Refer to SF case 116914 for Open Access
- Engineering was able to duplicate issue here.
- Somehow related to the main bus the PTP cards are plugged into- not due to the PTP cards themselves.
- Downgrading back to 5.5.1 or below temporarily fixes

**Report from John (28 Aug 17)** I've been trying to set up the PTP option cards, things like setting an IP address, mask, gateway.

An example IP setup: IP: 10.201.1.1 Netmask 255.255.255.0 gateway 10.201.1.1

The GUI gave me an error: Master Ip Error: Please supply a valid IP address.

So I thought I would clear-out the config and start fresh.

Check out the command output (from SSH session) below... "Failed to factory reset PTP Module" ?!

```
spadmin@pptp201 ~ $ clearstats
```

```
spadmin@pptp201 ~ $ clearlogs
```

```
spadmin@pptp201 ~ $ clean
```

```
PTP 0: Failed to factory reset PTP Module. Error=12 <br>PTP 1: Failed to factory reset PTP Module. Error=12 <br>PTP 2: Failed to factory reset PTP Module. Error=12 <br>PTP 3: Failed to factory reset PTP Module. Error=12 <br>PTP 4: Failed to factory reset PTP Module. Error=12 <br>PTP 0: Failed to factory reset PTP Module. Error=12 <br>PTP 1: Failed to factory reset PTP Module. Error=12 <br>PTP 2: Failed to factory reset PTP Module. Error=12 <br>PTP 3: Failed to factory reset PTP Module. Error=12 <br>PTP 4: Failed to factory reset PTP Module. Error=12 <br>spadmin@pptp201 ~ $
```

```
spadmin@pptp201 ~ $ clean
```

```
Exit: Fail to open logfifo
```

```
Exit: Fail to open logfifo
```

```
Exit: Fail to open logfifo
```

I can't use this system unless I can set the IP addresses and parameters on the PTP cards. None of the cards are taking a config as I'm getting errors setting the IP addresses.

---

## C) SIGTERM entry in the logs (such as Error\_log, SNMPD log, etc

### Update log entry

```
Jun 9 13:02:10 s43u1clk s43u1clk: [sw-upgrade] Upgrade Initiated, Reboot Required: /home/spectracom/update54A.tar.gz (SWUAL)
```

### Associated Error.log entries during a software update or halt

```
[Thu Jun 09 13:02:06 2016] [warn] [client 10.144.97.236] -authlogic- authtype is currently Pamacea (for /index.php), referer: https://s43u1clk.vida.local/Upgrades
```

Reboot required to complete upgrades.  
[Thu Jun 09 13:02:27 2016] [notice] caught SIGTERM, shutting down  
[Thu Jun 09 13:20:02 2016] [notice] Graceful restart requested, doing restart

### Associated SNMPD log entries during a software update or halt

Received TERM or STOP signal... shutting down...

### Associated SNMPD log entries during a software update

Jun 9 13:02:30 s43u1clk exiting on signal 15

---

## D) power cycling the unit (inadvertently or intentionally) before update is complete

**Email from Dave Sohn on 11/2/11**, regarding a customer power cycling SecureSync apparently before the update process had completed:

Remember that upgrade actually involves two reboots of the system. The first reboot is done into memory to rebuild the CF card with the new upgraded version. The unit then reboots again to start running from that newly built CF. During the first reboot, the front panel LCD will be blank, and the console is not available. If they power cycled before that process is complete, I would be concerned that something might not have been performed properly in the process. They may want to “force” another update at the same version to ensure that the upgrade completed fully and successfully.

**Software update when Skylight installed:** The upgrade process is the same, but they can only upgrade to other Skylight versions.

### Ability to perform software updates via CLI interface (for scripting updates)

- Version 4.8.8 (Dec 2012-ECN 3099) Added sysupgrade CLI command to perform software updates.

### Ability to perform a software upgrade via CLI command (instead of using the web browser), such as for scripting software updates

Starting in Archive software version 4.8.8, the software update can be initiated using a CLI command (issued via telnet, SSH or the front panel Serial port), instead of using the web browser, if desired. This entails performing an FTP/SCP transfer of the software update file into the SecureSync’s */home/spectracom* directory **and then issuing the *sysupgrade*** CLI command to initiate the software upgrade.

### Steps to upgrade the software using CLI interface

- 1) After extracting the .tar.gz update file from the file downloaded from our website, transfer the *updatexxx.tar.gz* update file into the time server’s **/home/spectracom** directory using an FTP program (such as Core FTP for instance)

- 2) Perform the **sysupgrade** command to initiate the update process.

The syntax for issuing the *sysupgrade* command is (where the “*updatexxx.tar.gz*” is the specific version upgrade bundle desired to be applied).

- Standard upgrade (Such as upgrading versions 4.8.8 to 4.8.9 for example): “sysupgrade” followed by the upgrade file name (Example: **sysupgrade update489.tar.gz**).
- Forced upgrade (Such as downgrading versions 4.8.9 to 4.8.8 for example, but can also be used with Standard upgrades, also): “sysupgrade force” followed by the upgrade file name (Example: **sysupgrade force update489.tar.gz**).
- Clean upgrade (Such as first performing a Forced upgrade from 4.8.8 to 4.8.9, for example. Then automatically resetting the NTP server back to factory default settings and deleting all log files): “sysupgrade clean” followed by the upgrade file



- name (Example: **sysupgrade clean update489.tar.gz**).

## A) Software issue after performing clean upgrade (with 5.8.2 and below installed) affecting TACACS log-in

- Symptom: Can access SSH via TACACS, but not the browser (applicable to versions 5.8.2 and below)
- **Per the v5.8.3 (Jan 2019) Release Notes** “Fixed an issue in which **clean updates** wouldn’t allow TACACS+ access through http”

---

### Software downgrade (using “force” update)

- Refer to the SecureSync software Upgrade Instructions (PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates) for specific information on performing software downgrades (not recommended to downgrade previous to version 4.8.6).
- It is not recommended to downgrade v4.8.6 (and higher), back to version 4.8.P (based on v4.8.5) and prior. The following httpd error message will occur when downgrading and the web browser may no longer be accessible (Refer to Salesforce case 6256).

```
spadmin@ELPICNTP02 sbin]$ ./httpd
httpd: Syntax error on line 1233 of /etc/apache/httpd.conf: Cannot load /usr/lib/apache/libphp5.so into server:
/usr/lib/apache/libphp5.so: cannot open shared object file: No such file or directory.
```

- Performing a Clean command after the force update appears to resolve this issue (Note: Clean command causes *an automatic reboot to occur*).

# Restrictions on/Recommendations for performing software downgrades to earlier software versions

## 1) Newer Maxim IC 7 Segment LED driver on front panel assy (~ Feb 2021):

- Cannot downgrade units with a Rev 13 front panel assembly to a software version **prior to v5.9.1**.

Refer to **ECO-FAI-2377** (in Arena): [https://app.bom.com/changes/detail-summary?change\\_id=2399381767](https://app.bom.com/changes/detail-summary?change_id=2399381767)

➤ Refer also to JIRAs **SSS-737** and **SSS-1042**

- **SSS-1042** discusses a couple available patches Engineering created for earlier versions (5.8.2, 5.8.4 and 5.8.J) to be able to work with newer hardware.

➤ Maxim IC LED driver (AS1116) was changed (due to discontinuance) to MAX7221 starting in **Front panel assembly Rev 13**. This newer IC required a software change to be incorporated. Previous Rev 12 doesn't have this change incorporated.

➤ Per Tom Ellison, downgrading to earlier software versions results in blank front panel

➤ **Per Dave West (3 May 2021)** The first serial number with the new chip would be 29427, but that doesn't mean we are at 100%"

- S/N 29427 shipped 2/10/2021

[10:20 AM] Tom Ellison  
589 paired OK with REV 12.

[10:20 AM] Tom Ellison  
589 does not like REV 13

[10:20 AM] Tom Ellison  
591 ok with Rev12 as well

## Associated Timing log entry asserted at every boot-up for new driver:

2000 001 00:00:01 000 Info: DP found AS1116 LED Chip.

---

## 2) Newer ETX module (SOM-4466) installed (~ Sept 2017):

➤ cannot downgrade unit with newer ETX module (SOM 4466) to a version **prior to v5.7.0**

---

## 3) uBlox GNSS receiver installed (as reported in the Interfaces -> GNSS 0 page of the browser)

- Cannot downgrade to a version **prior to 5.4.0/5.4.1** (~Mar 2016)

➤ Cut-in of ublox receiver for SecureSync/9400s: ~18 March, 2016 (S/N 11719, per Jill)

If you must run version 5.4.5, you can load the firmware and then make sure you select the "Force Update", "Perform Update" and "Clean Update" boxes in the update menu. This will ensure the downgraded firmware applies properly. Also, please note your configurations will go back to factory defaults so the unit will need to be setup just as a new unit would.

**If downgrading to a version of 5.5.1 and below, should install/reinstall hotpatch/cleaner due to SQLite database issue (should be reinstalled every time its downgraded to a version prior to v.5.5.1**

**Email from Dave L (12 Sep 17):** I would not recommend downgrading the firmware to version 5.4.5, but if you do, you should apply a patch after the downgrade, to prevent a firmware bug found in versions 5.4.1 and 5.4.5.

After the 5.4.1 update has been applied and the configurations setup, apply the attached firmware updateCleaner patch to resolve the bug I mentioned before. This patch should be applied to any Securesync

running version 5.4.1 firmware.

---

## Restore to factory defaults (vs Clean command)

**Email Keith Sent:** As for your great question about the difference between a “**Restore Factory defaults**” and a “clean/halt” (or the “clean” CLI command), these two processes are similar, but not exactly the same:

The “**Restore to Factory defaults**” procedure (which is directly “linked” to the software update process) is a much more “intrusive” process. It causes the Compact Flash (CF) card to first be completely wiped clean, before all files (in addition to the factory default configuration files) are then placed back onto the CF card, based on the upgrade bundle selected.

You can think of this process as being similar to reformatting a computer’s hard drive, and then re-installing the entire operating system. This is why the “Restore to Factory defaults” is directly tied to the software update process- so that it knows which version of software OS/Config files need to be put back onto the CF card, once the card has been completely wiped.

The “**clean**” command (which can be either accompanied by a HALT, or the unit booting back up afterwards) is just a reset of the specific configuration file values, back to their default settings for the version of software currently installed- if version 5.8.4 is installed, and a Clean is performed, just the config values are restored to the values they are in version 5.8.4 (the CF card is not first wiped, and files other than the configurations remain “untouched” during this process).

To just restore the settings to default values for the current software version installed, a “clean” CLI command or a clean/halt process is plenty sufficient. But, in cases such as a SecureSync operating in a military’s classified network, for instance, there is often concerns that someone may have transferred a non-Spectracom file onto the CF card,. A standard “clean” process (as it doesn’t first completely wipe the card clean) won’t remove any files not associated with its configs. If it’s not a config file, it’s not affected in any way by a “clean”. But performing a “Restore to defaults” instead, completely wipes everything which may be on the CF card at the time, and then completely reinstalls all files, as it applies to the update version bundle selected in the update dropdown field. Then, the entire CF card (not just the config settings) is exactly as it was initially shipped from the factory, for that version of software!!

---

## Update bundles being retained/deleted after update performed

- Software versions 4.8.9 and below (brutal linux): update bundles were retained after each update.
- Software versions 5.0.0 and above (Gentoo linux): update bundles are not retained after each update. They are automatically deleted (per Oleg, Gentoo hasn’t backed up/restored the update bundles).

---

## Software **upload** Failures (failure uploading the upgrade file into the server)

1. **Displayed error message of “500, internal server error” / “internal server error 500”**
  - Refer to Mantis case 3092 (Increase maximum speed Apache limits file download/upload)
  - Has been observed with update versions 5.3.0 and 5.3.1.
  - Likely partially caused by slow transfer rates due to encryption of data when logged in as HTTPS and Apache throttling back uploads so that it can still also be used as a browser during the upload.
  - Recommendation when this issue occurs- login with HTTP (instead of HTTPS) or manually upload the file using FTP/SFP (instead of using the browser to upload the file). Then use the browser (or the CLI) to initiate the upgrade.
  - v5.4.0 is lengthening the Apache timeout (30 seconds to 150 seconds) so that once 5.4.0 has been installed, this won’t be a potential issue for subsequent updates.

### **Draft email Keith uses:**

Some customers have observed a general error message when using the web browser to upload the software upgrade bundle file into the time server.

The error message is due a combination of a couple of factors, including the size of the upgrade bundles, the

Apache browser limiting the speed of the file upload so it can continue being a “browser” at the same time and the strengths of the cyphers algorithms that are encrypting the file as its being uploaded into the NTP server. So the file transfer is timing out in the browser before it can be fully uploaded.

There are a couple of easy work-arounds available for this condition. After rebooting the unit to clean out its /tmp directory (after each time the file doesn't fully upload, it leaves files behind in this directory):

- 1) If you don't need to have a secure connection to the SecureSyncs browser to upload the file (closed network for instance), login to the browser using HTTP instead of HTTPS (note that this may require HTTP be enabled in the server if it's currently disabled. Then the file will be transferred faster, and no longer time-out.
- 2) If you need a secure connection to upload the file, use an SCP file transfer program to put the full update file into the **home/spectracom** directory. Then use the browser as normal to initiate the update itself. Unlike the Apache upload, SFP/FTP don't throttle back the file transfer. These programs keep sending it as fast as possible without concerns of also having to “allot” resources for other simultaneous functions. This will also allow the file to be transferred before timing out.

With the file update file now successfully uploaded without timing out, initiate it using the browser – just like normal!! Among other changes implemented in the version 5.3.1 upgrade, it has lengthened the Apache timeout for file loads to help with future updates that may be applied.

---

## \*\*Software Upgrade Failures (failures after starting the update process)

### ➤ Review update log via either browser or the CLI interface

Possible reasons for upgrade failure:

- Corrupt update file (verify the md5 checksum of the file using a utility such as md5checker)
- CF card is too full (**df -h** command's response is greater than about 72%)
- Too many previous update files retained (try deleting all previous files)
- Via CLI interface
- To check for any previous updatexxx.tar.gz bundles via CLI: in the home/spectracom directory, type **ls -l** <enter>
- **To delete an update bundle** in the **home/spectracom** directory as spadmin account **rm <filename>** <enter>
  - for example: **>rm update594.tar.gz** <enter>

To delete an update bundle type **rm <filename>** <enter> (for example: **>rm update594.tar.gz** <enter>

**spadmin** account does have permission to delete “.tar.gz” files uploaded via the browser.

**-bash: syntax error near unexpected token `('**: To delete a “duplicate” update bundle file (a file name having a number inside of parentheses, such as “**update594(1).tar.gz**”), don't just type the file name verbatim. This will result in “**-bash: syntax error near unexpected token `('**” and the file not being deleted.

```
spadmin@Securesync12 ~ $ rm update595(1).tar.gz
-bash: syntax error near unexpected token `('
spadmin@Securesync12 ~ $ -bash: syntax error near unexpected token `('
> ls
```

- Instead, put the file name in quotes at the beginning/end, or type “**rm u**” and then press tab. This will auto-populate the file name and also add a couple of “/” characters, as well. Then, the rm command can be successfully performed.

```

spadmin@TestHostname ~ $ rm "update595(1).tar.gz"
rm: remove write-protected regular file 'update595(1).tar.gz'? y
spadmin@TestHostname ~ $ ls
broadshield-5.7.6.tar.gz  cert.csr  customize  log  update  xfer
cert                    config    default    mibs  update595.tar.gz
spadmin@TestHostname ~ $

```

```

spadmin@TestHostname ~ $ rm "update595.tar - Copy (2).gz"
rm: remove write-protected regular file 'update595.tar - Copy (2).gz'? y
spadmin@TestHostname ~ $ ls
broadshield-5.7.6.tar.gz  cert.csr  customize  log  update  xfer
cert                    config    default    mibs  update595.tar.gz
spadmin@TestHostname ~ $

```

- Not selecting **“Force Update”** when downgrading to an earlier version
- Temp directory has lots of files in it (such as due to past failed software updates or using TCPDump). Either Reboot or power cycle to clean out this directory.

**Update log entry indicates “[sw-upgrade] Upgrade Initiated, Reboot Required: home/spectracom/update517.tar.gz (SWUA)”**

- Observed with 5.1.4 to 5.1.7 update
- Should be fixed with 5.1J beta/ version 5.2.0 software update.
- Refer to Salesforce case 16749 (Jump Trading)
- Unit doesn’t complete the upgrade because it can’t reboot.
- Reboot commands via browser/CLI don’t work.
- Requires a hard power cycle of the unit to finish the update.
- Dave Sohn noted this has been observed with Verizon likely due to the potential pipe software command issue in 5.1.7 and below. “This sounds similar to the Verizon issue as well. I believe when we had an issue with one of the units, the hung process prevented the reboot. In that case, it took a hard power cycle to recover it.”

**General troubleshooting of a failed software update (specific failures futher below)**

- View the Update and System logs to see what they show (both can be viewed in the browser).

| UPGRADE STATUS  |             |             |        |           |
|-----------------|-------------|-------------|--------|-----------|
| Upgrade Failure |             |             |        |           |
| Package         | Old Version | New Version | Action | Status    |
| Application SW  | -           | -           | -      | Analyzing |
| Timing SW       | -           | -           | -      | Analyzing |

If **“Upgrade Failure”** is displayed during the update process or for some reason the upgrade/downgrade process doesn’t work:

- 1) If updating from versions 4.8.9 and below, what upgrade version is being applied? Note there is a check to ensure 5.0.2 has been installed before going to any versions beyond v5.1.2 (If you try applying 5.1.2 to 4.8.9 for example, the update will fail).
- 2) Look at the entries in the Update log (**Tools -> Logs** page of the browser). They will likely indicate why the update didn’t take.
- 3) Perform a **dh -h** CLI command with telnet or ssh (or look at the **“Disk Status”** menu in the browser starting in version 5.2.1 (bottom-left corner of the **Tools -> Upgrade/Backup** page)



- 4) If the CF card usage is greater than about 72%, delete the logs and NTP starts, delete previous update bundle files, reboot or power cycle to clear out the temp directory. Verify the usage drops.
  - To check for any previous updatexxx.tar.gz bundles via CLI, type **ls -l** <enter> (in the home/spectracom directory)
  - To delete an update bundle type **rm <filename>** <enter> (for example: **>rm update594.tar.gz** <enter>)
- spadmin** account does have permission to delete “.tar.gz” files uploaded via the browser.

- **-bash: syntax error near unexpected token `('**: To delete a “duplicate” update bundle file (a file name having a number inside of parentheses, such as “**update594(1).tar.gz**”), don’t just type the file name verbatim. This will result in “**-bash: syntax error near unexpected token `('**” and the file not being deleted.

```
spadmin@Securesync12 ~ $ rm update595(1).tar.gz
-bash: syntax error near unexpected token `('
spadmin@Securesync12 ~ $ -bash: syntax error near unexpected token `('
> ls
```

- Instead, either put the file name in quotes at the beginning/end, or type “**rm u**” and then press tab. This will auto-populate the file name and also add a couple of “/” characters, as well. Then, the rm command can be successfully performed.

- With versions 5.1.5 and below, need to use the cleaner patch to make space:

- Engineering has created a patch called “updatecleaner.tar.gz” (17 Feb 15) that cleans out unnecessary files.
- Link to this patch in Arena: [https://app.bom.com/files/detail-summary?file\\_master\\_id=1236440967&file\\_id=1748872341&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=6242513546](https://app.bom.com/files/detail-summary?file_master_id=1236440967&file_id=1748872341&orb_msg_single_search_p=1&redirect_seqno=6242513546)
- This patch is intended for update versions 5.0.0 and above only.

## B) Two different locations to delete the logs in web browser.

1. Delete just the logs displayed in browser (Qual, Update, etc) but not the system logs in the background (such as kern.log, sys.log, etc)

**Management -> Log Configuration** page. Click the “**Clear All Logs**” button in the upper-left corner).

### Notes

1. The Clear All Logs” and “buttons were added in 5.2.1 (I believe). (bottom-left of the **Tools -> Upgrade/Backup** page)
2. But with at least software versions 5.2.1 and below, these two buttons in the browser don’t work (was fixed in 5.3.0). Have to use the cli **clearlogs** command to delete these items with 5.2.1 and below.

2. Delete all of the logs (both the ones in the background and the ones in the browser)

above- via the bottom-left corner of the **Tools** -> **Upgrade/Backup** page (click the “**Clear All Logs**” button).

**Notes:**

1. The **clearlogs** command clears all logs (ones displayed in the browser and the “system” logs in the background. But it doesn’t clear the ntpstats and discstats. (refer to clearstats).

**Software issue associated with deleting logs and NTP stats via the browser**

- With software versions 5.2.1 and below, the “Clear All logs” button and Clear Statistics button didn’t work
- Note the associated CLI commands work fine in both Models.
- Refer to Mantis case 3049. <http://cvsmantis.int.rolia.com/mantis/view.php?id=3049>
- Fixed in the version 5.3.0.

**C) Delete logs via CLI interface (telnet or ssh)**

- clearlogs command via and cli was added in version 5.1.5 (I believe).
- Verify the checksum of the update bundle in the directory it’s being uploaded from (not a directory it was downloaded to, prior to moving it to another directory).
- View the size of the update bundle in the home/spectracom directory and make sure it’s the same size as the original update bundle (if it’s smaller, antivirus may have stripped some of the file).

In the default **home/spectracom** directory, type “**ls -lh**” at the command prompt (note there is a space between the “s” and the “-lh”).

The total size of the update bundle is reported (in MB) to the left of the date in the “**updatexxx.tar.gz**” row (as shown below):

```
Spectracom spectracom # ls -lh
total 200M
-rw-r--r-- 1 spui root 104M Jul 17 14:15 update512.tar.gz
-rw-r--r-- 1 spui root 105M Jul 21 20:37 update514.tar.gz
```

---

## Specific examples of Upgrade Failure:

1. Trying to install a version prior to v5.7.0 (in order to downgrade to an earlier version) when a newer Model ETX module is installed (started shipping Sept 2017) results in the following error in the Upgrade log:

“Down-grade using the file /home/spectracom.update545/tar/gz is not compatible for a 64-bit machine. Only versions at or above 5.7.0 are compatible. (SWUAL)”

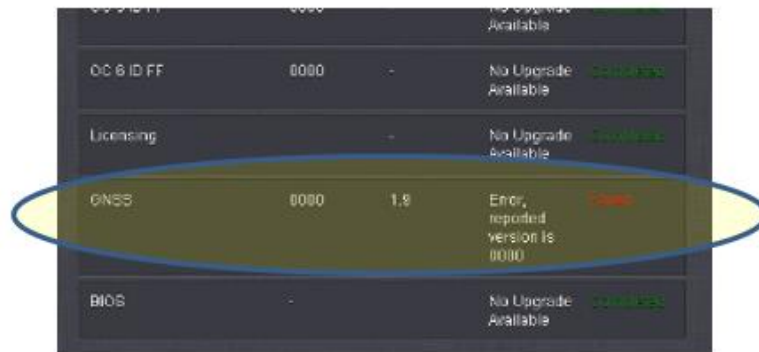
- Starting in software version 5.70 software, Paul M added a check to see if a newer ETX is installed, and if an earlier version of software is attempted to be applied, the updater will fail with an error message. The upper-right corner of the screenshot shows this error message!!



2. “Starting up System” remains indefinitely displayed on front panel LCD during (and after) attempted update

- Refer to Salesforce case 25112 (occurred during v5.6.0 update)
- Due to CF card’s writes/erases being “used-up”

3. “Error, reported version is 0000, Status: Failed” appears “Upgrade Status” ‘In Progress’ window (for “GNSS”)



- This Error message is due to having a Res-T GPS receiver (first Model used in SecureSync/9400s) installed when the v5.6.0 and above updater checks to see if a Res-SMT-GG or ublox is installed.
- No further actions required. There are no available/expected updates for the Res-T receivers.
- Hendrik intends to add note starting in the v5.7.0 update instructions.

**Email from Paul (18 Apr 17 after a v5.6.0 update attempt)** Thanks, I did not catch that ... You are right, the receiver does NOT support update is a Trimble Resolution T (RES T) not SMT. We can try to squelch that in a future release but it is not a priority now.



---

## SWUAL\_Lock: lockfile exists

Q I have been trying to "clean update" and Securesync unit but the software update is stalling part way through ... I have left it for days and it never finishes. I've power-cycled the unit and tried to update again (to 5.5.1) but the updater complains "Lock file exists"

I have been trying to "clean update" and Securesync unit but the software update is stalling part way through ... I have left it for days and it never finishes. I've power-cycled the unit and tried to update again (to 5.5.1) but the updater complains "Lock file exists. Is there a way to clear-out the lock file and get the update going again?"

```
spadmin@pptp201 ~ $ sysupgrade clean update551.tar.gz
Background upgrade process is running...
The process may take some time based on system configuration.
The system will reboot to complete the upgrade process.
Check the update log for status.
spadmin@pptp201 ~ $ SWUAL_Lock: lockfile exists
```

A Refer to Salesforce case 24121. Likely due to a full CF card. Perform a **df -h** CLI command

(note from Keith) Seems even more likely the unit just needs to be rebooted (a reboot fixed the issue with a later customer). Perhaps this is related to the /tmp file getting full due to earlier update attempts failing.

---

## 4. CF card too full to perform a software update (especially with earlier versions such as 5.0.2, 5.1.2, 5.1.4, etc)

- Engineering has created a patch called "updatecleaner.tar.gz" (17 Feb 15) that cleans out unnecessary files.
- Link to this patch in Arena: [https://app.bom.com/files/detail-summary?file\\_master\\_id=1236440967&file\\_id=1748872341&orb\\_msg\\_single\\_search\\_p=1&redirect\\_segno=6242513546](https://app.bom.com/files/detail-summary?file_master_id=1236440967&file_id=1748872341&orb_msg_single_search_p=1&redirect_segno=6242513546)
- This patch is intended for update versions 5.0.0 and above only.

---

## 5. Can telnet/ssh in after update, but can't access the web browser

- Refer to Mantis 2795 <http://cvsmantis.int.rolia.com/mantis/view.php?id=2795>
- First try just restarting Apache with **servset 6 on** / **servset 6 off**. Then try logging in again.
- If still not working, try resetting the HTTPS certificate using either the **defcert** or **defcert -sha1** cli command.
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - An example defcert CLI syntax (5.6.0 and above only) is **defcert -sha256**
  - V5.6.0 also changed the default algorithm to **SHA256** for better security (the default in 5.5.1 and below was SHA1) .
  - As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access to IE8 and below

**Email from Keith (20 Jul KW)** One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can't use this newer cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

---

## 6. Downgrading to an earlier version of software without select the "Force Update" checkbox, in addition to

## selecting the “Update System.

- Software downgrades or to same version require “Force Update” to also be selected.

## 7. Not enough room in CF card

- Issue CLI command **df -h** to determine CF card disk usage.

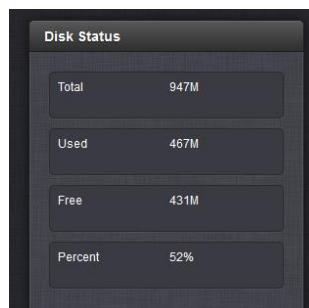
```
upadmin@Spectracom ~ # df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M  53% /
/dev/hda1       963M  480M  434M  53% /
devtmpfs        248M   0    248M   0% /dev
```

## CF card usage is now reported in the browser (alleviating need to have to use CLI command)

**Note:** Update version 5.2.0 added CF card memory status to the newer web browser (not available in classic interface).

**Note:** Also added ability to delete logs and Statistics from the same location

Tools -> Upgrade/Backup page of the browser (under “Disk Status”)



**Note:** In general, disk usage should be **less than** around **70%** or so usage to prevent issues with the update process. Logs and previous update bundles may be taking up too much space.

- Delete previous update bundles (such as update489, for instance) to free space
- Delete logs to free up space.
- Reboot/power cycle to clear out the temp directory (just in case it has lots of files in it)
- May or may not cause “Error (-1) Failure while unpacking Upgrade Bundle” / “Problem unpacking NWP bundle” to be asserted.

## Update log entries “Error (-1) Failure while unpacking Upgrade Bundle” / “Problem unpacking NWP bundle”

### LOG FILES

Timestamps are in system timescale (UTC)

| Event                                                                                                                | Alarms | Oscillator | GPS Qualification | NTP | Journal | Authentication | Update | Timing | System |
|----------------------------------------------------------------------------------------------------------------------|--------|------------|-------------------|-----|---------|----------------|--------|--------|--------|
| Nov 11 17:15:50 PSC-SecureSync PSC-SecureSync: [sw-upgrade] SW Upgrade Error (8) (SWUE)                              |        |            |                   |     |         |                |        |        |        |
| Nov 11 17:15:49 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE) |        |            |                   |     |         |                |        |        |        |
| Nov 11 17:15:49 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Problem unpacking NWP bundle (SWUE)           |        |            |                   |     |         |                |        |        |        |
| Nov 11 17:14:51 PSC-SecureSync PSC-SecureSync: [spupdate] Starting Update (SWUE)                                     |        |            |                   |     |         |                |        |        |        |
| Nov 8 22:35:22 PSC-SecureSync PSC-SecureSync: [sw-upgrade] SW Upgrade Error (8) (SWUE)                               |        |            |                   |     |         |                |        |        |        |
| Nov 8 22:35:21 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)  |        |            |                   |     |         |                |        |        |        |
| Nov 8 22:35:21 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Problem unpacking NWP bundle (SWUE)            |        |            |                   |     |         |                |        |        |        |
| Nov 8 22:34:26 PSC-SecureSync PSC-SecureSync: [spupdate] Starting Update (SWUE)                                      |        |            |                   |     |         |                |        |        |        |

### Likely causes:

- A) Corrupt update file. Run MD5 checker to verify file integrity
- B) Too many Update Bundles stored in unit.

### 1. Issue CLI command **df -h** to determine CF card disk usage.

```
spadmin@Spectracom ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M  53% /
/dev/hda1       963M  480M  434M  53% /
devtmpfs        248M    0  248M   0% /dev
```

In general, disk usage should be less than around 70% usage to prevent issues with the update process. Logs and previous update bundles may be taking up too much space.

### 2. Delete previous update bundles (such as update489, for instance)

To delete earlier update file, select each one in the drop-down, check only the **“Delete Update File”** checkbox in the screen where you normally select **“Update File”**. Then press Submit.



### 3. Then select **“Update System”**.

See if it proceeds through the process this time (as I suspect it will).

#### A) **Downgrading from 4.8.M to earlier version**

- Update log contained **“Spectracom Spectracom: [sw-upgrade] Downgrades require clean update: /home/spectracom/update488.tar.gz (SWUAL)”**

**Email from Dave Sohn (15 May 13)** **“In any case, the upgrade failed because 4.8.M to 4.8.8 is considered a downgrade and as of 4.8.9 (or M) downgrade requires the clean setting:”**

**Note:** **“clean update”** is not available in web browser, login using telnet/ssh and perform a **sysupgrade clean 4xx.tar.gz** command (where xx is the **“downgrade to”** version) as shown below:

```
Telnet 10.2.100.61
Linux 2.6.15-USAGI <spectracom.int.oriolia.com> <0>
Spectracom login: spadmin
Password:
Spectracom NetClock 9483 Version 4.8.M
spadmin@Spectracom ~$ sysupgrade clean update488.tar.gz
Background upgrade process is running...
The process may take some time based on system configuration.
The system will reboot to complete the upgrade process.
Check the update log for status.
spadmin@Spectracom ~$
```

[spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)

- Likely due to a problem with the update file in the unit- not likely a problem with the update process.

- 1) Check the MD5 file checksum to ensure the file wasn't corrupted when it was downloaded.

- 2) Make sure that if the file is being transferred in using FTP/SCP (instead of using the browser), that the file is transferred using "**binary**" mode. Otherwise, the file can be altered/corrupted during the file transfer.

---

## \*\*License files (for Purchased Options)

- License Install instructions: Refer to <..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\License Files Updates>
- License Files allow options such as Glonass, Skylight and Rinex server to be added in the field.
- The same license file that is used to enable Glonass is the same file used to enable Skylight phase 2/

### Creating license files

- 1) See Dave Lorah or Ron Dries for process to create files.
- 2) Licenses are **Model** and **Serial Number** specific:
  - Make sure Model is correct (“NetClock” or “1200”)
  - Make sure Serial Number is verbatim of what is programmed into the unit (**Tools-> Upgrade/backup** page). If here are no leading 0s in the Serial Number, do not use a leading 0 when creating the license file.

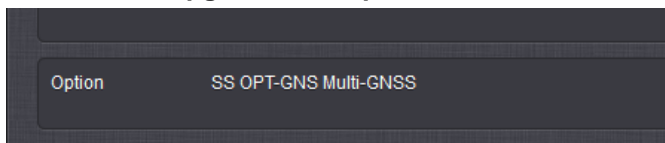
### Viewing installed license files

**Note:** Also in newer firmware version 5.7.1 and higher units, the “**manifest**” command will show all the system information in more detail.

To view installed licenses/options:

#### A) Via web browser

Go to **Tools -> Upgrade/Backup**. Scroll down to the bottom of the **System Configuration** table.



#### B) Via CLI

The CLI command is “**options**”

```
spadmin@Spectracom-226 ~ $ options
1:IRIG 2324:Gb PTP
2:Gb Eth 5:PPS TTL
3:485 RLY6:None
```

### Deleting license file

Deleting license file from the browser doesn't remove the Option- just the file used to enable the Option.

### Troubleshooting license file install

- Licenses are Model and Serial Number specific:
- Model Number (NetClock or 1200) matters (as reported in the **Tools -> Upgrade/Backup** page)

#### Leading “0” in Serial Number matters (as reported in the Tools 0> Upgrade/Backup page)

- If there is one or two leading 0s in the Serial Number, the license has to be created with the 0.
- If there is no leading 0s in the Serial Number, the license has to be created without the 0.

**\*\*\*SC037 (“Trade and Industry Department Cryptography Questionnaire”)/Blowfish**

**SC037 (“Trade and Industry Department Cryptography Questionnaire”)/**

➤ Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Cryptography questionnaire>

**Blowfish (part of the Crytography questionnaire referred to above)**

**Email from Paul Myers (29 Jun 17)** “BlowFish is in OpenSSL but I don’t know how we use it.

Why is blowfish marked specifically.  
I don’t remember what uses it.

|                                                                                                     |                                     |                                     |
|-----------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| (1) A “symmetric algorithm”                                                                         | <input type="checkbox"/>            | <input type="checkbox"/>            |
| If “yes”, please state the following:                                                               | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| (i) Full name <u>blowfish</u> :                                                                     | <input type="checkbox"/>            | <input type="checkbox"/>            |
| (ii) Key length <u>128 conf</u> bits;                                                               | <input type="checkbox"/>            | <input type="checkbox"/>            |
| (iii) It is used for authentication only;                                                           | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| (iv) It is used for digital signature only;                                                         | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| (v) It is used for execution of copy-protected software only;                                       | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| (vi) It is used for encryption or decryption of data file<br>(including image, voice or text etc.); | <input type="checkbox"/>            | <input type="checkbox"/>            |
| (vii) Other application: <u>Key management</u>                                                      | <input type="checkbox"/>            | <input type="checkbox"/>            |

**System initialization after each boot-up**

System outputs default time of 00:00:00 (incrementing) year 2000 while initializing

Q. (From Jennifer Trotta with Raytheon) I have a question about time code output when the SecureSync is rebooted due to a configuration or other change. Does the IRIG output ever put out all zeroes when the system is going through a reboot? What happens to the IRIG signal upon reboot?

We are seeing some squirrely behavior on one of our units downstream that is receiving the IRIG signal. It thinks that the year rollover has occurred when we do a reboot.

**A Reply From Keith Wing (7 Aug 2014)**

To answer your question, as the SecureSync is booting-up and loading, it will initially output the time as all 0’s (and the year as the default of 2000), and then start to increment the seconds value from there, each second. The estimated time is typically loaded into the timing system for it to update the outputs (such as IRIG) within about a minute or so after applying power, or after performing a reboot.

This start-up initialization of the system can be viewed very easily by power cycling the SecureSync and then watch the green LED clock on the front panel. Moments after power up, the time will be displayed (such as 00:00:02, by the point it can be displayed) and then it increments the seconds once-per-second. This continues for just over a minute. Then the System clock (which controls the date/time to the outputs such Perf as IRIG) is corrected by the Real Time Clock, which continues to maintain an estimate of the time/date while the system is powered down. The front panel time display and the system outputs such as IRIG, will jump to this estimated time, until an input reference (such as GPS) becomes present and valid, at which time the date/time is corrected as needed and the Sync LED turns green.

The method to prevent the initialization of the SecureSync from needing to occur is to keep it continuously powered-up.

---

## Third-party software packages used/not used in SecureSync

### A) systemd

- Per <https://en.wikipedia.org/wiki/Systemd>

**systemd** is an init system used in Linux distributions to bootstrap the user space and manage all processes subsequently, instead of the UNIX System V or Berkeley Software Distribution (BSD) init systems. It is published as free and open-source software under the terms of the GNU Lesser General Public License (LGPL) version 2.1 or later.<sup>[5]</sup> One of systemd's main goals is to unify basic Linux configurations and service behaviors across all distributions.<sup>[6]</sup>

- Per Dave Sohn (5 July 17, pertaining to CVE-2017-445) **"We do not currently use systemd on SecureSync"**

---

### Anti-virus software (antivirus software)

Q (from TOYO) Our customer NTT East who are considering introducing your time servers newly, they have a question about anti-virus policy of the product. Could you please answer their questions below?

1. What measures are prepared against threat of computer viruses in the SecureSync?
2. Is it possible to install an anti-virus software to the SecureSync?  
(If yes, do you have any recommendation?)
3. If the SecureSync has no specific measures, please tell us your policy and the grounds.

**A Reply from Dave Sohn (28 Jul 17)** The SecureSync is not a general application server. It is a purpose-built appliance. While it utilizes a standard operating and file system, it is not susceptible to viruses in a similar way as a general purpose machine, and as such does not include anti-virus SW or provisions to run anti-virus SW. Vulnerabilities are minimized through the security mechanisms built-in. The ability to inadvertently load and execute malicious code that can compromise the system is limited based on customer privilege levels (no root access). In addition, system SW updates are verified through hashing and checksums to prevent manipulation of update images.

## Front Panel / keypad

### \*\*Front panel connections

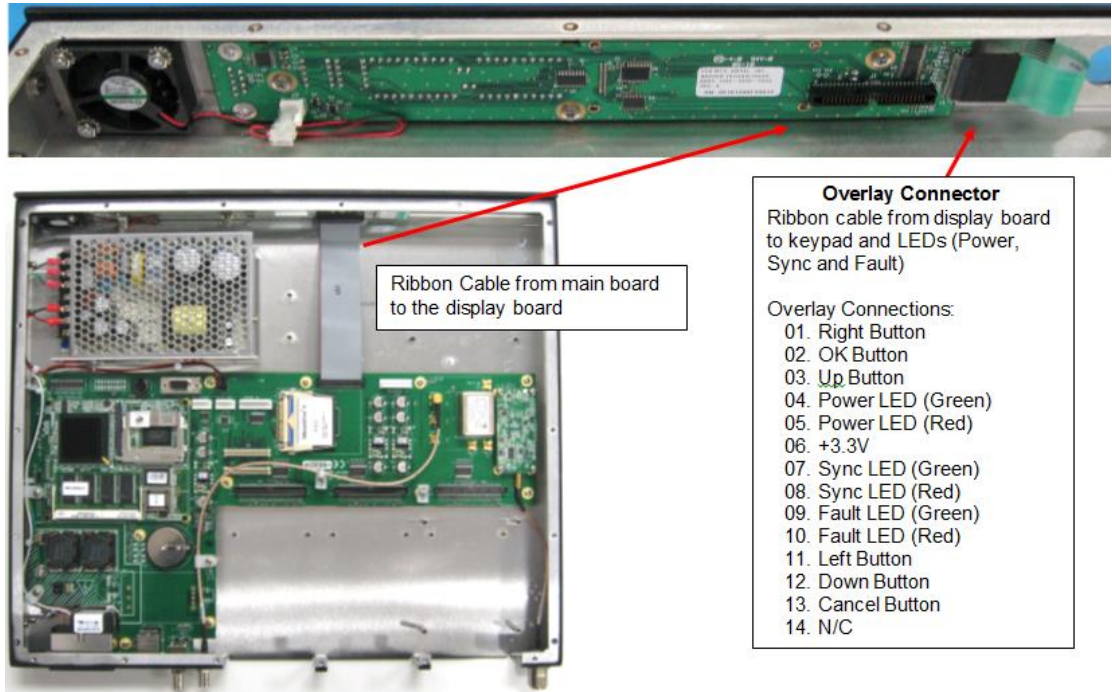
#### Schematic for SecureSync

- **Front panel PCB board** (1200-1001-0300) (in 1200-0000-F004) in Arena:

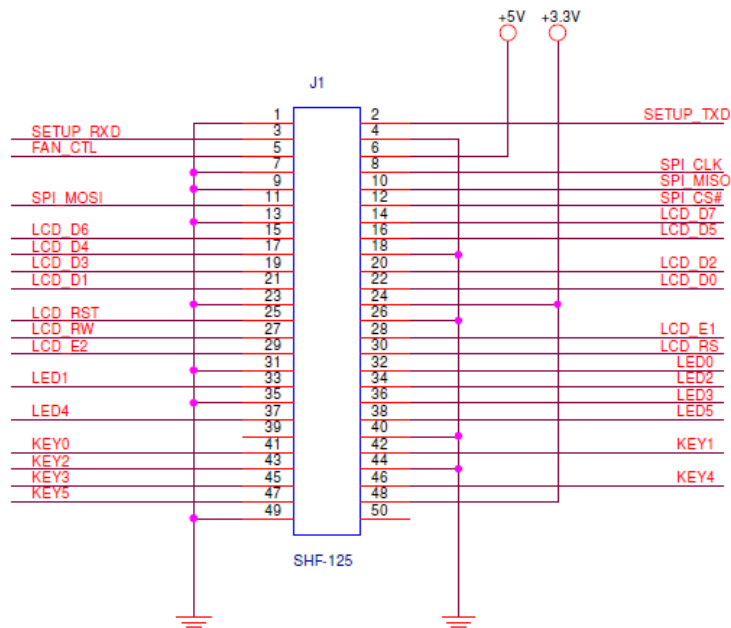
[https://app.bom.com/items/detail-spec?item\\_id=1202839909&version\\_id=10299091328&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=8027520292](https://app.bom.com/items/detail-spec?item_id=1202839909&version_id=10299091328&orb_msg_single_search_p=1&redirect_seqno=8027520292)

- **Main SecureSync PCB board** (1200-1001-0200) (in 1200-0000-F003) In Arena:

[https://app.bom.com/items/detail-spec?item\\_id=1202839908&version\\_id=10290528958&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=8027522349](https://app.bom.com/items/detail-spec?item_id=1202839908&version_id=10290528958&orb_msg_single_search_p=1&redirect_seqno=8027522349)



### Main Board I/O





## \*\*Front Panel LCD / LED time display / keypad



### LED Time display while the system is initially booting-up (after power cycle, reboot or clean)

During boot-up (power-up or reboot), or after a clean, the displays are initially all blank. After a few moments, the LED display goes to all 0's for several seconds. Then, it displays the time read from the RTC (which should be fairly accurate). Then later, the LCD will start displaying data, also (unless the front panel is configured for "None" in the front panel "Display Content" field).

- The front panel time display, like other outputs such as IRIG and ASCII, will initially output the default year 2000 and the time as 00:00:00 (incrementing each second) for about the first minute or so after power -up. Then the time/date is applied.
- For more details, refer to: System initialization after each boot-up in this document
- As of at least Apr 2015, version 5.2.1, the only way to prevent this is to not reboot.

#### Email from Sylvain to Dave Sohn

Q. The issue : When the SECURESYNC is rebooting : the IRIG output is distributing during the BOOT period many different times values.... changing.... Amazing ... ? These false information are very unpleasant for the displays units which are connected to the outputs of the SecureSync. Version of the SecureSync : 4.8.6.

#### Dave Sohn responded (18 Oct 2012)

When KTS powers up, the default state of signals is enabled. As the NWP powers up, it performs any of the persisted settings of the user including signature control, formats, etc.

### LCD display component

- Component Ref Designator: **DS9**
- Our P/N: **DS20R-G001-0H00** (DISPLAY, LCD,122X32,GRAPHIC,GRN,FFSTN,6:00)
- **Mfg and MFG P/N:** Hantronix: HDM32GS12L-S-KKLS

Link to Data sheet:

<https://files.bom.com/download/NqbBR8vPMrQpDrggaa83Uc7BUbePRyM3/jwcgrgdokszfocozfkmwrksibjlswdmh/Hantronix%20HDM32GS12L-S-KKLS.pdf>

---

## API calls associated with Front panel display

- Refer to Tim Tetreault's "cheat sheet" at: ..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet
- These are examples - additional calls may have since been added

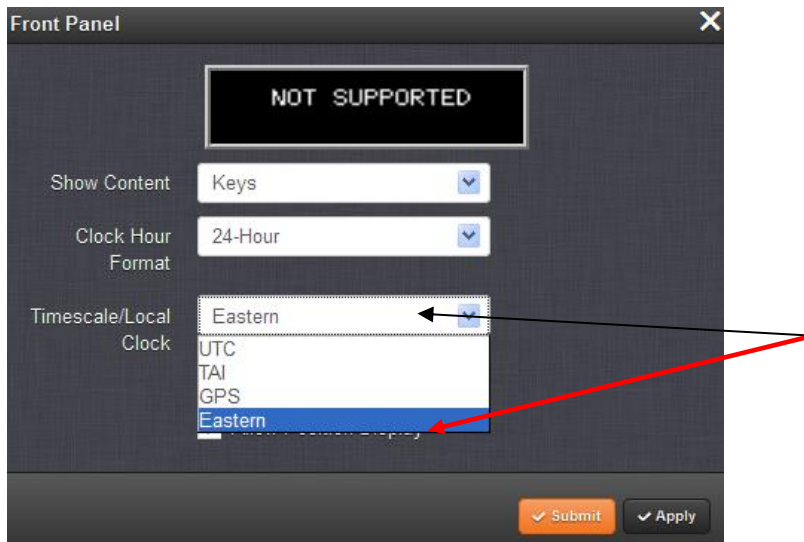
| <b>Front panel display commands</b> |
|-------------------------------------|
| DP_GetFormat                        |
| DP_GetLocal                         |
| DP_GetNumInst                       |
| DP_GetTimeScale                     |
| DP_SetFormat                        |
| DP_SetLocal                         |
| DP_SetTimeScale                     |

| <b>LED CONTROL Commands</b> |
|-----------------------------|
| EC_GetMode                  |
| EC_GetState                 |
| EC_SetMode                  |
| EC_SetState                 |

\*\*\*Configure front panel LED clock (and clock in web browser) to display local time

A) New web browser (archive versions 5.1.2 and higher)

Management -> Front Panel page



Software issue with web browser displaying a one hour time error (front panel cLED clock is correct)

- Update software version 5.2.0 fixed a DST issue with the web browser displaying a one hour time error, if the front panel is configured to display local time.

Two different decimal points in front panel LED time display (when its configured to display local time)



- **DST indicator:** The decimal point to the right of the minutes indicates the front panel clock is showing a Local Clock time AND Daylight Savings Time in in affect. This is a Daylight Savings Time indicator.
  - **PM indicator:** The decimal point to the right of the Hours portion of the clock display means the front panel is showing a Local Clock time in 12 hour mode AND the time is PM. When the time transitions to AM the decimal point will extinguish.

Q I have noted since installation of release 5.8.0 a new LED symbol illuminates after the SecureSync is up and running. Note the separator decimal point lower right of the minutes digit lit. I contacted Dave Lorah at Spectracom and he noticed this as well on his rack. A search of the manual does not reveal any answers.

A reply from Dave L (4 Jun 18) I have found the decimal point to the right of the minutes characters in the clock display indicates the front panel clock is showing a Local Clock time AND Daylight Savings Time in in affect. This is a Daylight Savings Time indicator.

When we transition out of Daylight Savings Time in November the decimal point will extinguish.

The decimal point to the right of the Hours portion of the clock display means the front panel is showing a Local Clock time in 12 hour mode AND the time is PM. When the time transitions to AM the decimal point will extinguish.

I was able to locate this information in our online User Manual. So this will be included in the next pdf revision of the manual

**Note:** With Timescale configured as "Local" and during DST (Daylight Saving Time, as configured in the Local Clock), a "DST indicator" (decimal point) will be displayed to the bottom-right of the minutes portion of the LED time display. The "DST indicator" extinguishes during "Standard" time. If the Local Clock is configured as "No DST/Always Standard Time", the DST indicator won't ever be lit.

---

### \*\*\*Configure/display network settings using the front panel keypad/LCD

- Note that the IP Address of Eth0 is automatically displayed on the front panel by factory default (though another menu may have been configured by a user to be displayed).
- Refer to online SecureSync user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm?Highlight=Enable%20eth](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm?Highlight=Enable%20eth)

#### To enable/disable Ethernet interfaces via front panel keypad (Not applicable to version 5.5.1 and below)

- Update version 5.6.0 added ability to enable/disable Ethernet interfaces via the front panel keypad.
  - 1) Press the green checkmark on the front of the unit. This will display the main menus.
  - 2) Press the white right arrow keys on the front to highlight “**Netv4**”.
  - 3) Press the green checkmark.
  - 4) Press the white right arrow keys on the front to highlight “**eth?**” (Eth0, Eth1, Eth2, Eth3)
  - 5) Press the green checkmark.
  - 6) Then, use the up or down arrow keys to scroll to **Port**”.
  - 7) Press the green checkmark.
  - 8) Press the green checkmark to enable the port, if its currently disabled.

#### To verify or change network settings via the front panel keypad, if not already displayed in the LCD

- 1) Press the green checkmark on the front of the unit. This will display the main menus.
- 2) Press the white right arrow keys on the front to highlight “**Netv4**”.
- 3) Press the green checkmark.
- 4) Press the white right arrow keys on the front to highlight “**eth0**” (or Eth1, Eth2, Eth3)
- 5) Press the green checkmark.
- 6) Then, use the up or down arrow keys to scroll to “**IP Addr**”.
- 7) Press the green checkmark.
- 8) The top row (next to “O=”) displays the currently assigned IP address for this Ethernet interface. The letter at the end indicates if DHCP is enabled (D) or if DHCP is disabled for a static address (S).

#### To change the IP address to a desired static address (Starting from step 8 above)

- 1) Press the “X” on the front of the unit to go back to the **Home/NetV4/“Eth?”** menu.
- 2) Use the up or down arrow keys to scroll to “**DHCP**”
- 3) Press the green checkmark to disable DHCP
- 4) Then, use the up or down arrow keys to scroll to “**IP Addr**”.
- 5) Press the green checkmark.
- 6) Using the arrow up/down arrows to change the value and right arrow to sequence to the next placeholder, configure the bottom row (next to “N=”) to the desired P address for this Ethernet interface. Using the up or down arrows, change the “/xx” value at the end to the applicable subnet mask for the network

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

Table 2-2. Subnet mask table

7) Press the green checkmark twice to accept.

## Configure eth0 via keypad with NO network cables connected to the unit (0.0.0.0 will be displayed)

- “0.0.0.0” will inherently be displayed, making it appear as though the network settings are being lost upon reboot, though the settings are not being lost.

Refer to online SecureSync user guide at:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm)

### Your most recent response

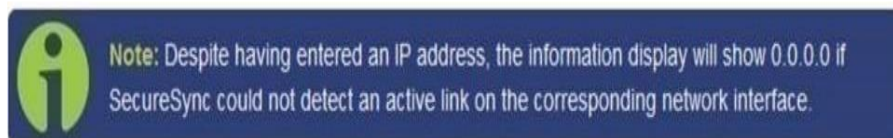
Are you saying that THE ONLY WAY to pre-configure a SecureSync device (with a basic IP, subnet and gateway) is to connect the Eth0 interface to a network?

This does not make sense at all. What is the purpose of the serial port connection, and/or the front panel configurator? We configure many type of devices on a daily basis, including Ciscos, Junipers, F5, Firewalls, WAPs, etc, and they all can be accessed/configured via a console port, regardless if they are connected to a network. Plus I don't see anything on the instructions on the Spectracom link, indicating so. Perhaps I am not understanding your request, so I ask you kindly to provide further instructions on how to proceed, as at the moment, I can't connect it a live network.

### My response

Please do understand that you DO NOT need any network connections at all to pre-CONFIGURE eth0 with its intended network settings. You can simply use the Front panel keypad/LCD (as shown in the following screenshots) to successfully configure eth0 (and these settings WILL persist subsequent reboots). There is no need to have a network cable connected at any time to CONFIGURE eth0.,

But if you wish to **view** the settings you have entered, a network cable needs to be connected (to have the front panel display those settings, or to login to the browser to view the settings in the browser, if you wish)// As indicated in the SecureSync user guide note below (from [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm)) the front panel will not DISPLAY the network settings which have been configured in ETH0, unless or until a network cable has been connected to eth0 and another network device. NOTHING has to be done using this network cable. Eth0 just needs to sense that there is an active network connection for eth0 to stop displaying the built-in indication (network addresses being reported as 0.0.0.0 on the front panel) when eth0 is detecting there is no network cable currently connected. This DISPLAY of all 0s lets users know that the port is not connected to another network device (such as its network cable not being plugged in). Moments after a cable is connected to eth0, the port realizes it now has a cable connected and will then continue to display the network settings it was previously configured with (even if the SecureSync was rebooted after the settings were made).



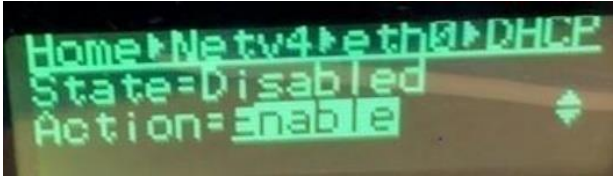
As “pictures are worth a thousand words”, I just performed the same eth0 configuration steps (using only the front panel LCD/Keypad) I understand you are also performing.

Until noted further below in these steps, there were NO network cables connected to the SecureSync)

- 1) I first verified DHCP for Eth0 is set to Disabled (State=Disabled)



- 2) I configured the intended IP address for eth0



- 3) I configured the intended gateway address for eth0



- 4) Front panel "Show" menu indicates I have successfully configured eth0 with a Static IP address (DHCP is not enabled), as indicated by the "S" to the right of the IP address. ("Unplugged" indicates there is still no network cable connected to eth0)



- 5) I then power cycled the SecureSync (blank display is shown while its rebooting)



**After booting-up (still no network cable connected to the SecureSync)**

- 6) The **Show** and **eth0 IP address configuration** menus are reporting addresses as all zeroes, BECAUSE THERE IS NO NETWORK CABLE CONNECTED TO ETH0"



### A Network cable was just now connected to eth0

- 7) I then **just connected a network cable from eth0 to a small switch sitting on my desk**. Within just a couple moments of connecting this network cable, the screen automatically refreshed to display the same network settings I had configured before the unit was rebooted. (all I did was connect eth0 to another network device, to clear the built-in indication (all 0s) that lets a user know a cable is not connected to that network interface (such as eth0))



- 8) I then just disconnected the network cable connected to eth0 to show what is displayed every time the interface doesn't detect its connected to another network device (after boot-up or during routine operation without a reboot). Within just a couple moments of disconnecting the cable from eth0, the display automatically changed back to the built-in indication (all 0s displayed for the port not having a cable connected) to let me know there is no cable currently connected to eth0 again (note this is the same display which was present when I first booted-up with no cable connected)"



In summary, as long as there is an "S" displayed after initially configuring eth0 via the front panel, DHCP is disabled and the static IP address HAS been successfully configured (and these settings are not being lost after reboot). There is no need to connect a cable to configure eth0. But if you wish to see the settings did persist/save during the reboot, just optionally (not required for successful configuration) connect an ethernet cable to eth0 and another network device (PC/HUB/Switch), to temporarily clear the built-in indicator of eth0 sensing that there is no currently no cable connecting it to its hub/switch. This indicator clears just a couple moments after the network connection to eth0 is in place!

I hope this information helps illustrate the settings of eth0 are NOT being lost upon reboot

### LCD is configured to be blank when not pushing any keypad buttons (standby mode)

The LCD can be configured to display different items (such as network settings). One of the choices is "None". When this menu option is selected, the LCD will not show anything, except for when any of the buttons on the keypad (other than the "X" key, as normal) is pressed (any of the arrows and the checkmark will display the menu again). Then, it will go back to blank again (it goes blank again about 1 minute after the last time a key is pressed).

If "None" is selected when the system is cleaned/rebooted, "Stopping System" will still be momentarily displayed on the LCD (as normal) as the system is rebooting.

### To change this display option to any other value (so that it's always displaying data):

- **From the front panel:** hit any button to go into the menu. In the Home menu, select "Display" and then use the up or down arrows to select any other display option.
- **From the web browser:** Navigate to the **Setup -> Front panel** page. Change "Display Content" field to anything other than "None" and Submit. The change takes effect immediately.

## Front panel Menus that can be displayed in LCD window

### \*\*Front panel Config storage (screenshots below from v5.8.9)

- Front panel configurations (except local clock) are stored in the **fpmcf.config** file located in home/spectracom/config directory

**lccf.config: just the local clock settings** (example below configured for East coast/auto DST)

#### lccf.config

```
spadmin@Spectracom ~/config $ cat lccf.conf
50 0 2 0 0 Eastern
spadmin@Spectracom ~/config $
```

**lcdf.config (lists all created local clocks and their settings)**

```
spadmin@Spectracom ~/config $ cat lcdf.conf
Pacific 0 -28800 0 3 2 0 2 11 1 0 2 3600
Eastern 0 -18000 0 3 2 0 2 11 1 0 2 3600
spadmin@Spectracom ~/config $
```

See below

0= don't rotate menus  
1= rotate menus

0= don't lock keypad  
1= keypad locked

```
pfactory@Spectracom / $ cd home/spectracom/config
pfactory@Spectracom ~/config $ ls
agpps.conf  gpsrinxd.conf  nesf.conf      ofdf.conf
ardf.conf   ktsif.conf     notcf.conf     pwdcf.conf
pmpcf.conf  lccf.conf      ofdf.conf      relay.map
pscf.conf   lcdf.conf      ofdf.conf.bak  rnmf.conf
pfactory@Spectracom ~/config $ cat fpmcf.conf
content 1
rotate 0
spLock 0
position 1
rotateSecs 5
```

**Content field** - determines which menu to display on the LCD

| Content | Display                        |
|---------|--------------------------------|
| 1       | Network (eth0) factory default |
| 5       | Status                         |
| 6       | Position                       |
| 7       | Day of Year                    |
| 8       | GNSS                           |
| 9       | Date                           |
| 10      | Keys                           |
| 11      | None (blank screen)            |

- Which LCD menu to display is selected in the:
  - **Newer browser** (v5.1.2 and above): [Management](#) -> [Front panel](#) page
  - **Classic Interface browser**: [Setup](#) -> [Front Panel](#) page of the ("Display Content" field)
- The same information shown on the front panel is also reported with the **gpsat** CLI command.
- Software version 5.0.0 removed the Mobile mode Dynamics value. So, only "Mobile" is displayed when the GPS receiver is in Mobile mode and it's currently tracking satellites.
- Reports "**Acquire**" when not tracking any satellites (no matter which mode the receiver is in)



## “GPS” menu

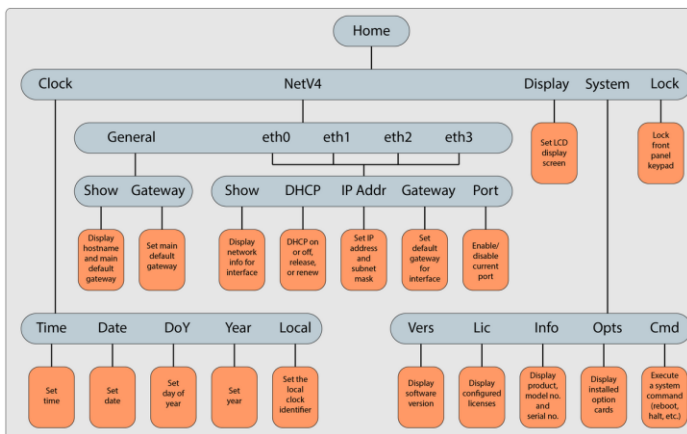
```
[spadmin@Barrett_SideB ~]$ gpssat
GPS SPS 123456789ABC
Max 47 | | | | | | | | | |
#Sat 9 | | | | | | | | | |
Station | | | | | | | | | |
```

- Refer to **gpssat** CLI command in SecureSync CLI section for additional info on this menu)
- Refer also to “Reviewing the GNSS Reference Status” section of the Model 1200 online user guide at: [https://orolia.com/manuals/SS/Content/ Global/Topics/GNSS/View\\_GNSS\\_Ref\\_Status.htm](https://orolia.com/manuals/SS/Content/Global/Topics/GNSS/View_GNSS_Ref_Status.htm)

## Rotate Menus

- Pressing front panel button stops front panel display rotation (Mantis case 1792)
- If rotate front panel displays is enabled and the user locks the display, then presses a Submit button and possibly any button the front panel display stops rotating on the next screen.

This is by design. An internal timeout of 60 seconds is started on key press causing the screen to freeze when in rotation. Normally it would switch to a menu waiting for user input. There is no reason to change this behavior. Rotation resumes in 60 seconds. The key press allows a user to pause the display for evaluation.



## LCD/Keypad

**Home/Management (mgmt) menu:** (as of 11/9/2010) This displayed menu was initially for controlling management capabilities of the Ethernet ports. The desired method of control was changed and this value was supposed to be removed from the front panel. But it hasn't yet been removed. This menu has no functions assigned to it and a Mantis case is open to remove it from the front panel.

**Note:** the “**mgmt**” command was also listed in the CLI and has since been removed. cli Refer to Mantis case 1423 (command was removed in version 4.5.0).

Refer to [Management/Network Access restriction](#) (further below) for more information on Management/access control.

---

## Keypad frozen/not responding or very sluggish

- A frozen keypad not operating can be caused by a few conditions:
  - A) **Keypad may be locked** (refer to info below to try unlocking the front panel, OR navigate to the Management -> Front panel for the field that allows the panel to be locked/unlocked)

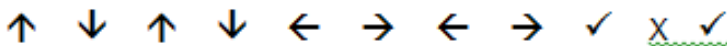
### If Keypad is unlocked and still not working

- Likely a **bad ETX module or oscillator failure**- assign an RMA for return (Search system.log for "**oscillator**" and "**fpga**". These entries being present indicate likely bad/failing oscillator).
- Keypad not responding/sluggish menus can also be caused by **Denial of Service attack- excessive network traffic/heavy NTP** loading, or **heavy malicious packets** being sent (as in Salesforce Case Number 207952- they have an outside team come in to test their network security to see if they can break it or gain unauthorized access. They were sending thousands of SSH requests to the SecureSync, for example)

---

## \*\*Front panel keypad lock/unlock

If front panel is locked the following sequence will unlock it:



This sequence must be completed quickly (within 5 seconds, I believe) or the front panel won't unlock.

Q. Is there a way to lock the front panel that can't be re-enabled by entering the key sequence listed in the manual on the front panel?

**(Sam Otto to a customer 11 Jul 2013)** We don't have a way to turn off the Keypad unlock routine.

## Desire for more secure locking mechanism

Q This brings a security problem as anybody can force the unit manually though the keypad and modify the network properties for example...

**A Per Dave S (1 Jun 17)** The keypad lockout is to prevent accidental and casual changes using the front panel. Our view is that the customer is responsible for physical security.

## Ability to lockout position data in LCD:

Version 4.8.6 (June 2012) adds a field in the **Setup -> Front Panel** page to disable position from being displayed in the front panel LCD.

---

## Front panel FAQs

Q Does the front panel have any sort of security/protection such as entry of credentials or password to gain access to certain functions?

**A.** The front panel does not utilize credentials or password. The keypad can be locked, but can be unlocked via the web UI or entering in a preset pattern on the keypad.

Q Is the GPS lock status displayed on the front panel? Is it possible to determine whether or not the GPS receiver is operating in SAASM mode via the front panel (specifically, indication of using PPS versus SPS)?

A GPS status can be displayed on the front panel. It will display PPS vs SPS mode.

**\*\*Front panel status LEDs (AC and DC power monitoring)**



**Front panel Status LEDs are bi-color LEDs (Green on top and red at the bottom)**

**Q.** I have an NTP server that may have a faulty power module. The power light blinks red but not full on red, it's like the bottom half of the light is only lighting up. The sync under it is solid green so it couldn't be that like bleeding over into the power light above it.

**A. Email Keith Sent to a customer** Note that the three status LEDs for the SecureSync are bi-color LEDs, with a small red LED on the bottom and a small green LED on the top. When the antenna is connected and the unit first powers up (or an alarm other than the Antenna Problem alarm is asserted thereafter), just the red LED at the bottom of the Fault LED will turn on, causing the whole LED to be lit solid red, though the bottom of the LED will be slightly brighter than the top of the LED.

However, if the SecureSync's GPS/GNSS antenna is not attached, or if a GPS splitter is used to share an antenna, the Antenna Problem alarm may be asserted. This alarm, with no other alarms asserted, will cause both the red LED at the bottom of the Fault LED and the green at the top of the Fault LED to simultaneously blink to generate an amber color Fault LED. Note this is the same operation of the Sync LED when the unit enters Holdover mode. With the antenna disconnected and the unit in Holdover, both the small red and green LEDs in the Sync LED will be continuously lit, resulting in amber color Sync LED. In both cases, if you look very closely at the flashing Fault LED you will notice a "brighter red spot" towards the bottom and a "brighter green spot" towards the top. These are the two internal LEDs being lit and not a carry-over from the green Sync Led above.

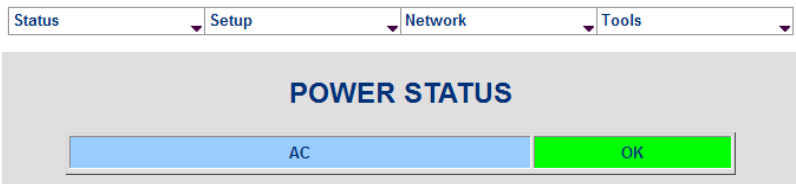
- Power:** Green, always on.
- Sync:** Tri-color LED indicates the time data accuracy.
- Fault:** Indicates equipment fault.

At power up, a quick LED test is run which illuminates all three LEDs. The following table provides an overview of the LED status indications:

| Label | Activity        | Description                                                                                                                                                                                                                                                                                       |
|-------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power | Off             | Both AC and DC Input Power are disconnected. Or, SecureSync's AC input switch is turned off and DC input is not present.                                                                                                                                                                          |
|       | On              | AC and/or DC Power are supplied and SecureSync is energized.                                                                                                                                                                                                                                      |
| Sync  | Red             | Time Sync alarm. 1) SecureSync has powered up and has not yet achieved synchronization with its inputs. 2) SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs were declared invalid) and the Holdover period has since expired. |
|       | Solid green     | SecureSync has valid time and 1PPS reference inputs present and is synchronized to its reference.                                                                                                                                                                                                 |
|       | Orange          | In Holdover mode. SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs are not declared valid). SecureSync's outputs will remain useable until at least the Holdover period expires.                                              |
| Fault | Off             | No alarm conditions are currently active.                                                                                                                                                                                                                                                         |
|       | Blinking orange | GPS antenna problem alarm has been asserted and is currently active. A short or open has been detected in the GPS antenna cable. The light will automatically turn off when the alarm condition clears (Refer to Section 9.4 for troubleshooting this condition).                                 |
|       | Solid orange    | A Minor alarm condition (other than an antenna problem alarm) has been asserted and is currently active (Refer to Section 9.1.2 for troubleshooting this condition).                                                                                                                              |
|       | Red             | A Major alarm condition has been asserted and is currently active (Refer to section 9.1.1 for troubleshooting this condition).                                                                                                                                                                    |

**Table 1-1: Front Panel Status Indicators**

## Status/Power page of the classic interface browser



- Version 4.8.0 and below showed both AC and DC indications, whether or not both were installed (power option not installed was automatically displayed as red alarm state).
- Starting in version 4.8.2, this web page now only displays which power configurations are installed (if an AC or DC power configuration isn't installed, it's not displayed in the browser).

### POWER LED flash pattern

Starting in update 4.8.2, the Power LED will indicate status of input power (ECN 2861):

If the Power Indication is Off: Both AC and DC Input Power are disconnected. Or, SecureSync's AC input switch is turned off and DC input is not present.

If the Power Indication is Green, but blinking Orange once per second; Indicates power error condition; general power configuration fault.

- GREEN w/ **ORANGE BLINKING**: Power fault; Power inputs don't match configuration
- ORANGE SOLID – DC ONLY – DC only power detected; AC & DC supported
- ORANGE SOLID – AC ONLY – AC only power detected; AC & DC supported
- GREEN SOLID: All configured power is present

**Note:** Green/amber flashing indicates the SecureSync or NetClock was not originally programmed as the correct Model type during the manufacturing process (indicates configuration issue).

#### Email from Dave Sohn (3/16/12)

If the SecureSync is setup for dual power (AC / DC power) with firmware **version 4.8.2** or higher, the power LED only flashes orange if the unit isn't configured properly. If there is a failure on a power supply, the power LED will be solid orange.

**Email Keith sent to a customer (2 Jan 2013)** - I saw your email to Jeremy regarding the blinking orange Power LED on the SecureSync and have some information for you that I hope will help!

FYI- During the manufacturing process, the SecureSync is programmed with its particular input power configuration (such as AC only, or AC and DC input, for examples). This particular SecureSync was likely inadvertently programmed with the incorrect power configuration, resulting in the blinking orange that you are observing. When programmed correctly and with an input power not applied, the LED will be solid orange, instead of blinking orange. Blinking orange only occurs if the power configuration isn't programmed correctly.

In archive versions prior to version 4.8.2 (as reported in the **Tools** - > **Versions** page of the browser), there were no alarms associated with input power being present or not present. So even if the SecureSync happened to be programmed incorrectly, there was no visible indicator for this condition. However, if a SecureSync is updated to a version of 4.8.2 or higher, since version 4.8.2 adds an indication of lost power via the Power LED, an incorrect programming will then become apparent.

This blinking power LED does not affect the operation of the SecureSync. If this is a demo SecureSync that you currently have, thanks for bringing this to our attention. We will fix it when its returned to us. However, if this is a SecureSync you have already purchased, please let me know. if you can connect the SecureSync to the internet, outside of a firewall, and provide us with the IP address (and enable all Services) we can reprogram it remotely for you, to resolve this issue. If it can't be temporarily placed on the Internet, we can also assign an RMA Number for it to be returned for a reprogramming. Or, we may be able to work with our engineering team to provide you with a special upgrade file that can also reprogram it in the background.

### \*\*\*Ability to mask/override the Power LED/Power alarm (if backup power is not connected)

(5 Apr 2013 KW) Currently (as of at least versions 5.8.5 and below), there is no way to mask/override the Power LED alarm pattern if SecureSync has both AC and DC input configuration, but only one power source is connected.

- Refer to Salesforce case 9038 and Mantis case 1983.

#### Available work-arounds to inherently clear this Power alarm condition (if AC is supplied and no DC power is applied, for instance)

##### 1. Apply a special Software hotpatch to alter the Power configuration of the unit

- Make the unit THINK it only has ONE power input instead of two
- this approach is more of a “permanent” solution than the next approach further below (it will take another patch to reverse it back to its original configuration)

##### 2. Some time ago, Ron Dries apparently created a special patch (for T-Mobile) to “mask” their missing power indications:

- Refer to “special patches” in this doc: [Special software patches](#) and the folder (“Disable Power Fault with dual input power”) at: [..\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\Specials\software patches\Disable Power fault with dual input power](#)

##### 3. Sometime later (Oct 2019), another special patch was created by Ron Dries (for Rhode & Schwartz) to “mask” the missing power indications

- Refer to SF case 210981
- Refer also to “special patches” in this doc: [Special software patches](#) and the folder (“Disable Power Fault with dual input power”) at: [..\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\Specials\software patches\Disable Power fault with dual input power](#)
- **Details of this case:** Customer had both AC and DC input installed in the SecureSyhn, but was only using AC input only (not using the DC input). So Ron created a special patch for them, which reconfigures the unit to be “AC only” (will no longer check to see if DC power is present) **“Attached is a patch that will set the model number to 1200-033 which is AC only.”**

## OR

##### 1. Purchase our **PS06-2Z1M-DT01** (external AC to DC converter) to provide “DC input” via “dual AC”



- Purchase from us and connect the available external AC to DC converter (Our P/N “**PS06-2Z1M-DT01**”) to the DC connector on the back of the SecureSync (thereby applying power to both connectors).
- this viable solution can be either temporary or “permanent”, with no changes needed to be applied to the timeserver (unlike the other solution of applying a software patch, which changes the unit)
  - Refer to (in this document) “**PS06-2Z1M-DT01**” for more info on this available power adapter.

Q On some GPS-Clock, we did not connect the DC Power, on the GPS-Clock, the DC Power appears in red and monitoring system generates an alarm. Is there a way to configure the Spectracom GPS-Clock to inform it that the DC Power is simply not plugged in (look like a check box)? Currently we have an unjustified alarm and we don't want to handle exceptions.

**A reply from Keith (2 Feb 17) There is no way to clear/mask the DC power alarm with a SecureSync having either of the two input power connections not having power applied.**

However, if a customer purchased a unit with both AC and DC input, but isn't planning on applying DC

input power, we offer an available AC to DC converter, that can act as a redundant AC input (and thereby inherently clearing the Power alarm indication, when its connected). This external AC to DC converter has a DC connector that mates with the DC connector on the back of the time server, for convenience (as shown below). Our P/N for this available adapter is PS06-2Z1M-DT01:



---

### Sync LED

If the Sync Indication is **Red**; Time Sync alarm. 1) SecureSync has powered up and has not yet achieved synchronization with its inputs. 2) SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs were declared invalid) and the Holdover period has since expired.

If the Sync Indication is **Green**; SecureSync has valid time and 1PPS reference inputs present and is synchronized to its reference.

If the Sync Indication is **Orange**; In Holdover mode. SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs are not declared valid). SecureSync's outputs will remain useable until at least the Holdover period expires.

### Fault LED

If the Fault Indication is **Blinking orange**; GPS antenna problem alarm has been asserted and is currently active. A short or open has been detected in the GPS antenna cable. The light will automatically turn off when the alarm condition clears

If the Fault Indication is **Solid orange**; A Minor alarm condition (other than an antenna problem alarm) has been asserted and is currently active

If the Fault Indication is **Red**; A Major alarm condition has been asserted and is currently active

---

## Known Issues/Conditions associated with front panel LCD/ LED time display/front panel ribbon cable

### A) Newer Maxim IC 7 Segment LED driver on front panel assy (~ Feb 2021):

- Cannot downgrade units with a Rev 13 front panel assembly to a software version **prior to v5.9.1**.
  - Refer to **ECO-FAI-2377** (in Arena): [https://app.bom.com/changes/detail-summary?change\\_id=2399381767](https://app.bom.com/changes/detail-summary?change_id=2399381767)
- Refer also to JIRAs **SSS-737** and **SSS-1042**
  - **SSS-1042** discusses a couple available patches Engineering created for earlier versions (5.8.2, 5.8.4 and 5.8.J) to be able to work with newer hardware.
- Maxim IC LED driver (AS1116) was changed (due to discontinuance) to MAX7221 starting in **Front panel assembly Rev 13**. This newer IC required a software change to be incorporated. Previous Rev 12 doesn't have this change incorporated.
- Per Tom Ellison, downgrading to earlier software versions results in blank front panel
- **Per Dave West (3 May 2021)** The first serial number with the new chip would be 29427, but that doesn't mean we are at 100%"
  - S/N 29427 shipped 2/10/2021

[10:20 AM] Tom Ellison  
589 paired OK with REV 12.

[10:20 AM] Tom Ellison  
589 does not like REV 13

[10:20 AM] Tom Ellison  
591 ok with Rev12 as wel

---

### B) Front panel LED time display one hour incorrect

- If a new CF card has been installed, make sure a software update was performed thereafter (to update KTS Timing software to the correct version)

---

### C) Front panel ribbon cable disconnected

---

### D) (Jan 2019) The header letter "c" for the 12<sup>th</sup> satellite in the GNSS signal strength bar graph is partially cut off at the right edge of the LCD display



- refer to Case 184367

**Email from Jodi (17 Jan 2019)** We did some research on this. I spoke directly with one of our Repair Techs as well. After speaking with Tom, we can say that the observation that you've made is normal, and the last digit being cut off could be due to an older firmware version for the display.

The display showing in this manner does not affect functionality or cause problems. We have seen this before, especially with older displays, that have the older firmware, and our own devices in the Tech Support Lab show the last digit "C" as cut off as



well.

If this is still a problem, you do have the option of sending in the device on an RMA and we can try to get a display with a more recent version of firmware installed for you, by our Repair Team. The turnaround time would be approximately 3-4 weeks. This would be at a cost, as this is not a warranty repair.

---

### E) (Oct/Nov 2014) LED time display is frozen. Seconds not incrementing

- Communications (HTTPS, SSH, etc) may be sluggish as a factor of KTS not responding.
- Indicates KTS (Timing System) is frozen/locked-up.
- Network processor software likely still OK.
- Likely due to loss of/glitch in 10MHz OCXO oscillator output adversely affecting the FPGA.

Refer to “**LED time not counting up. LCD is fine (OCXO glitching causes lockup)**” in the oscillator section of this document (Mantis case 2916)

- Review System log for **KTS failed to read log** entries (examples below). In versions 5.2.1 and above also look for “**possible oscillator error**” or “**probably FPGA Failure**” entries. These are associated with 10 MHz glitching issue mentioned above.

```
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GR_GetMfrMdl 0 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetState 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetOscType 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetSerialNo 0 (KTSAL)
```

- Bring back for oscillator evaluation.

---

### F) Front panel LCD window and Time display intensity matching (one unit compared to another)

**Notice:** The LCD protective film issue described further below only applies to the LCD window display. If the LCD window AND the Time display are at a different intensity than another unit, the issue further below does not apply.

Differences with both the LCD and Time display as compared to other units are due to tolerances in electronic components and the front panel filter.

**Below is a (now modified) email Keith sent to Mark Day in the UK about this (may need to be edited before sending to anyone else)**

Initially, there is a protective film on the front panel components that needs to be removed before the front panel assembly is placed in the front panel portion of the chassis. The intensity difference between two units may likely be due to this film inadvertently not being removed from one of the two units (one has this film removed and the other unit has the film still applied –resulting in one display being darker in appearance than the other.

To begin, the display intensities are not adjustable and we don't perform any side-by-side intensity matching of the front panel displays. However, typically the display intensity from one SecureSync to another is fairly similar. Any intensity differences between them are normally limited to tolerances of the electronic components (such as the intensity setting resistors) and the filtering of the front panel overlay.

Your customer can either remove the cover and the power supply that inhibits the front panel assembly from being removed, to see if the film is still applied to these components (if the film is still applied to one of the two, the bottom unit in the picture appears to be the one with the film still applied). OR, they can send the SecureSyncs back to us for evaluation.

---

### G) Front panel LCD protective film still installed when unit is received

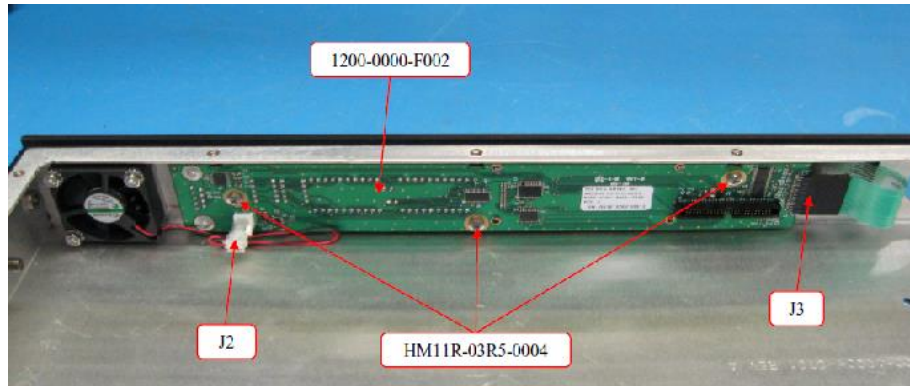
#### **Email from Dave Lorah to customer (6/12/12)**

We apologize for the problem with your new SecureSync unit. This has been recorded and preventive action is being addressed by our QA department.

Fortunately this can be easily fixed in the field. The front panel assembly will need to be detached from the Cd and chassis. All you need is a medium Phillips screwdriver.

**Here is what to do:**

- 1) Remove the 20 screws from the top cover and remove the cover.
- 2) Remove the fan connection shown as (J2) below.
- 3) Remove the three screws attaching the front panel PCB to the chassis. You may not need to remove the J3 or ribbon cable to get to the film.
- 4) The protective film on the LCD Display will peel off easily.
- 5) Reassembly is the reverse of disassembly.



If you have any questions or need assistance please let me know.

---

**H) LCD display dark after booting-up a cold unit (cold LCDs)**

**report from Sylvain to Dave Sohn** We recently made a experimentation outside on site and I had a little issue on SecureSync that I would like to share with you :

This was in the early morning, it was cold outside and the unit has spent the night in the back side of our car. At the first starting up time, I couldn't see the front panel display working normally : LCD remaining Black and LEDs Power Green only (others OFF) – I just could see the clock display keeping running then taking the RTC time after more than a minute. Then nothing else. After a second reboot (power OFF action): the SecureSync started as well.

**My question is:** as the firmware + software of my Securesync doesn't include the last BIOS configuration changing the threshold parameters for temperature limits, can it be corrected by this setting ? I assume it is not link to the high temperature this time but in cold status context....

**Reply from Dave Sohn (18 Mar 16)** LCDs at cold temperature may be blank and sluggish for updates. If the time display was running, LEDs were lit, and the time was updated from the RTC then I would say the SecureSync was running. When we do our tests that is what we see, but the LCD comes back after it warms up.

---

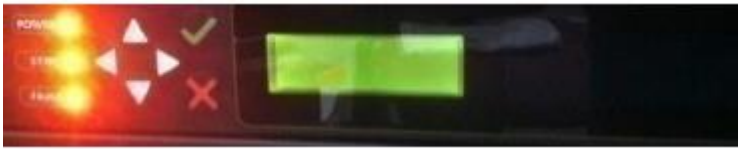
**I) LED time not counting up. LCD is fine (OCXO glitching causes lockup)**

**J) Only the Power LED is lit (LED time is NOT displayed and nothing is displayed in LCD either)**

**1. Issue with the oscillator/10 MHz into KTS Timing System**

**(email from Dave Lorah to a customer, 23 Jun 16)** If the clock is not working then I believe the oscillator has failed. That is the symptom of a failed oscillator, just the power LED and nothing else on the front panel.

## K) LED time is NOT displayed and nothing is displayed in LCD either. All LEDs lit



### 1. CF card is near or at 100% usage

### 2. Restarting/Rebooting the unit while its been running very warm

- This symptom can happen with Rb oscillator installed; if unit is rebooted/power cycled and it running really hot
- Check the internal temperature to see if it's running near upper recommended limit of 55 degrees C.
- This condition was fixed in the **version 5.4.0** software update (via BIOS changes to the ETX Module)

**Q. Email from Sylvain** Starting issue: when they switch OFF the unit (the unit was working well until this step) : if they start again the Power supply of the units (just few seconds after powering off) : the **unit never restart properly.**

Situation: the time information on the right panel (LED display) is not working and the Left display is only backlitged but with no indication. For ever. I have never seen this issue before. In general, the LED display is at least displayed even if the Left display shows nothing...

**Reply from Dave Sohn:** What is the temperature of the unit? I've seen this on units when we were testing at our highest end of our temperature specification.

### 3. No LED or LCD display (accompanied by Unable to open /dev/tsyncpci0: No such file or directory)

- "Unable to open /dev/tsyncpci0: No such file or directory Unable to open /dev/tsyncpci0: No such file or directory Unable to open /dev/tsyncpci0: No such file or directory Unable to open /dev/tsyncpci0: No such file or directory Unable to open The following error appears in the UI: "Unable to open /dev/tsyncpci0: No such file or directory"

Additionally, the system logs contain the following repeated messages:

```
Feb 23 14:39:46 Spectracom spectracom: [system] Failed to read alarm info from KTS (KAD)
Feb 23 14:39:46 Spectracom spectracom: [system] Failed to read sync state from KTS (KAD)
Feb 23 14:39:46 Spectracom spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 1] (KHTD)
Feb 23 14:39:45 Spectracom spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 1] (KHTD)
Feb 23 14:39:45 Spectracom spectracom: [system] Front Panel daemon has terminated (FPD)
Feb 23 14:39:45 Spectracom spectracom: [system] Front Panel daemon has started (FPD)
Feb 23 14:39:45 Spectracom spectracom: [system] Front Panel daemon failed to initialize LCD panel (FPD)
Feb 23 14:39:45 Spectracom spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)
Feb 23 14:39:45 Spectracom last message repeated 4 times
```

- Refer to Salesforce case 21277 (Google saw this on a very-early RB-based SecureSync)
- Only indicator on the front panel was the power LED (even after reboot).

## L) Front panel LCD is scrolling on its own

- We had a batch issue with IC U5 (July 2013)
- Refer to ECN 3294 for change to two resistor networks

I found a bad IC on the production SecureSync that was having front panel display problems this morning. The problem was the display was locked up during burn in. There were no errors in the logs. After I powered the unit down and moved it to my bench, the display started constantly scrolling through the menu as if one of the keys was being held down.

Assembly: 1200-0000-F002  
Component: U5 U050R-0541-000P

I found TWO of the lines coming from the keypad were not holding at 3.3V, but were down at 1.2V. Ohm meter check did not see any difference on the lines. It was only apparent when powered up.

The test points TP6 and TP11 were the particular lines.

I replaced U5 on the front panel board with a known good and it solved the problem. Looks like we may have a batch of bad IC's???

---

### M) Earlier issue with ribbon cable rubbing on metal

- Ribbon cable had tape applied and metal was removed (prior to July 2013)

---

### N) LCD is blank (menus not displayed) but LED time is incrementing normally

- Not likely an issue with the oscillator (osc can affect LED time display but unlikely to affect the LCD display)
- Likely an issue with either the ETX module or the CF card
  - Try reseating ETX module (which is needed for the LCD but not for LED time display)

#### Location of and reseating of ETX module

##### ETX should be reseated

**Email from Jodi to customer (28 Sept 17)** There is a possibility that the problem could be that that ETX module is not fully seated within the SecureSync. Are you able to—do you have permissions to—remove the cover and press down on the center of the ETX module to make sure it's fully seated? If so, I can send more information on that.

**Email from Jodi to customer ( 28 Sept 17)** The ETX module is located near the CF card. It has 4 screws and a black heat sink. Remove power from the Secure Sync first, of course. Once you remove the cover of this SecureSync, we recommend following best practice for ESD environments. Remove the screws from the ETX module, take the module out, then re-seat it and replace the screws. Once you've ensured that it's fully seated, you can then put the cover back on and start the device up again.

- Refer to Salesforce case 10148 <https://na8.salesforce.com/500C000000RbG0E>

---

### O) Front panel keypad not responsive

- Keypad may be locked. Try unlocking it via either the web browser or from the front panel using the unlock sequence.
- If the front panel isn't locked, try power cycling the time server. May need to be returned due to issue related to the ETX or could be a software issue.
- This one isn't related to the 10MHz oscillator (which can affect the LED time display).

---

## **\*\*out-of-band management/Front panel DB9F SERIAL console Setup port**

### **Out of band management**

From Wikipedia ([https://en.wikipedia.org/wiki/Out-of-band\\_management](https://en.wikipedia.org/wiki/Out-of-band_management)) In [computer networks](#), **out-of-band management** involves the use of a dedicated [channel](#) for managing [network devices](#). This allows the network operator to establish trust boundaries in accessing the management function to apply it to network resources. It also can be used to ensure management connectivity (including the ability to determine the status of any network component) independent of the status of other [in-band](#) network components.

- SecureSync provides the front panel RS-232 Serial port for serial/terminal server connections to the CLI interfacer (see below for more info)

---

### **Front panel SERIAL port (console port)/Terminal server connection**

Refer to SecureSync online user guide:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/SS/Topics/INTRO/Specs\\_Serial.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/SS/Topics/INTRO/Specs_Serial.htm)

- DB9F connector (DCE device)
- Front panel Serial port is password protected (must login).
- Refer to CLI section directly below for info on commands.
- Login user names and passwords are same as used to login to the web browser.

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/SS/Topics/INTRO/Specs\\_Serial.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/SS/Topics/INTRO/Specs_Serial.htm)

#### **RS-232 Serial Port (Front Panel)**

**Function:** Accepts commands to locally configure the IP network parameters via CLI for initial unit configuration.

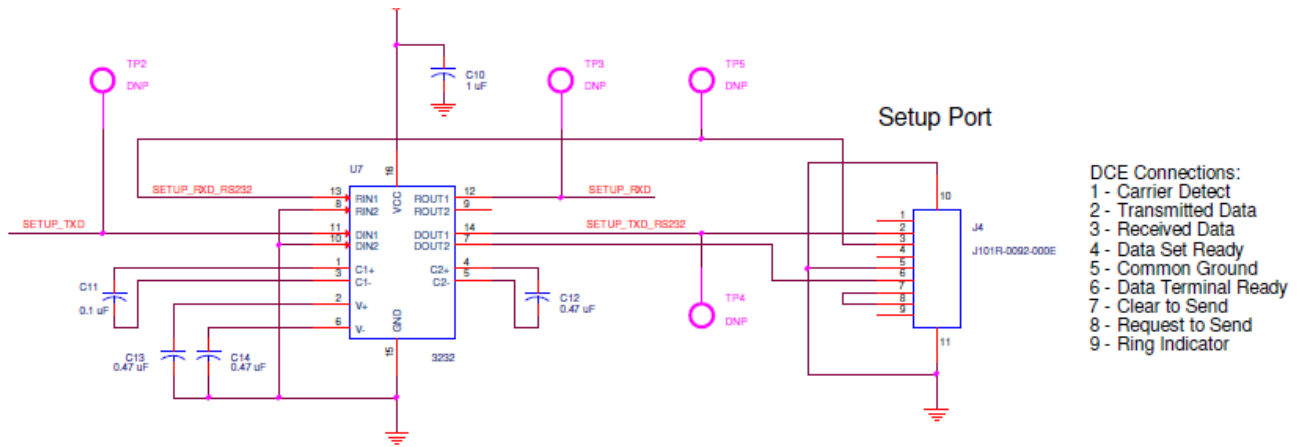
**Connector:** DB9 F, pin assignments conform to EIA/TIA-574, data communication equipment

**Character structure:** ASCII, 9600 baud, 1 start, 8 data, 1 stop, no parity

---

### **RS-232 signal levels/pin-out (DCE device)**

- RS-232 driver (U7 on Front panel PCB): U050R-3232-000P (Texas Instruments MAX323) in Arena: [https://app.bom.com/files/detail-summary?file\\_master\\_id=1237200855&file\\_id=1750108215](https://app.bom.com/files/detail-summary?file_master_id=1237200855&file_id=1750108215)
- 5v logic



### Connection time-out for Serial interface login

- there is no time-out/configurable timeout
- the Serial interface is considered a “physical security” interface – not a “network security” interface. Customer is responsible for maintaining security of this interface

**email from Morgan (23 Jan 19)** Unfortunately there is no timeout setting for the serial interface, it has very limited configuration capability.

### Ability to completely disable the RS-232 Console port (for enhanced security)

- as of at least version v5.8.6 and below (at least Sept 2019) console port cannot be disabled within the SecureSync
  - This falls under “**physical security**” of the SecureSync, which is the customer’s responsibility

Q is possible disable the console port on SecureSync server?

**A Keith’s response (27 Sept 2019)** : like the web browser login, access to the SecureSync’s Console port is also password controlled. There is no way, with the SecureSync itself, to disable the console port altogether, Blocking unauthorized access to the console port falls under physical security of the SecureSync chassis (such as placing the SecureSync in a locked room/locked cabinet. for examples) which is the customer’s responsibility to provide, as they desire/require.

## Interface Serial port with a Terminal Server/Cisco router's ASYNC/Console port (DTE device)

- Refer to SR 5457
- Refer to <http://www.cisco.com/c/en/us/support/docs/dial-access/asynchronous-connections/5466-comm-server.html> and <http://www.cisco.com/c/en/us/support/docs/routers/1600-series-routers/46789-port-pinout.html>

### Settings

9600, 8 bit, 1 stop bit, no parity, flow control off (must disable hand-shaking on their end)

### Pin-out

#### Notes

- When using an RJ-45 to DB9M, pins 2 and 3 need to be reversed on one of the DB9 cable (as shown below)
- On our end, we only care about pins 2, 3 and 5

below is from: <http://www.cisco.com/c/en/us/support/docs/routers/1600-series-routers/46789-port-pinout.html#db9>

**Console Port Signaling and Cabling with a DB-9 Adapter**

The next table shows the pinout descriptions for the DB-9 connections:

| Cisco router (DTE) | RJ-45-to-RJ-45 Rollover Cable |           | RJ-45-to-DB-9 Terminal Adapter | Console Device |
|--------------------|-------------------------------|-----------|--------------------------------|----------------|
| Signal             | RJ-45 Pin                     | RJ-45 Pin | DB-9 Pin                       | Signal         |
| RTS                | 1 <sup>3</sup>                | 8         | 8                              | CTS            |
| DTR                | 2                             | 7         | 6                              | DSR            |
| TxD                | 3                             | 6         | 2                              | RxD            |
| GND                | 4                             | 5         | 5                              | GND            |
| GND                | 5                             | 4         | 5                              | GND            |
| RxD                | 6                             | 3         | 3                              | TxD            |
| DSR                | 7                             | 2         | 4                              | DTR            |
| CTS                | 8                             | 1         | 7                              | RTS            |

<sup>3</sup>Pin 1 is connected internally to Pin 8.

| SecureSync console port (DCE) |                                               |
|-------------------------------|-----------------------------------------------|
| Pin                           | Signal                                        |
| 1                             | CD (Carrier detect)                           |
| 2                             | RXD (RS-232 output)                           |
| 3                             | TXD (RS-232 input)                            |
| 4                             | DTR                                           |
| 5                             | Ground                                        |
| 6                             | DSR                                           |
| 7                             | RTS (Note: pins 7 and 8 internally connected) |
| 8                             | CTS (See note above)                          |
| 9                             | RI (Ring Indicator)                           |

[http://www.showmecables.com/product/DB9-Male-RJ45-Female-Modular-Adapter-Kit.aspx?utm\\_source=google&utm\\_medium=cse&utm\\_campaign=15-109-160&gclid=Cj0KEQjwnIm7BRDSs42KxLS8-6YBEiQAfDWP6JQVqlbSm2rD5pIReLTi5IMD4gU4B5UbDeLofAMQ8claAul\\_8P8HAQ](http://www.showmecables.com/product/DB9-Male-RJ45-Female-Modular-Adapter-Kit.aspx?utm_source=google&utm_medium=cse&utm_campaign=15-109-160&gclid=Cj0KEQjwnIm7BRDSs42KxLS8-6YBEiQAfDWP6JQVqlbSm2rD5pIReLTi5IMD4gU4B5UbDeLofAMQ8claAul_8P8HAQ)



## Case Number 197156

### Your initial inquiry

I am looking for a serial adapter that will work with the NetClock 9400 series. It has the reverse gender of most of the adapters we have in stock and doesn't work with any of the pre-fab ones we have.

I need a way to plug a standard RJ45 serial cable in so I can connect the appliances to our console servers for remote access.

### My response (reply from Keith)

Though the NetClocks have the available Serial (RS-232) interface, this interface is not commonly used (since the CLI commands this RS-232 connector provides are also available via the NetClock's Ethernet interfaces using telnet/ssh- this ethernet connection is much simpler).

Connecting the standard -232 "Serial" port (a DCE device) on the NetClock to a computer requires either a standard DCE to DTE RS-232 cable, pinned straight-thru (to connect the NetClock to a serial adapter on the PC). Or, a if you wish to instead connect it to a network interface on the PC, requires a serial (RS-232) to Ethernet converter (RS-232 on the NetClock-end and ethernet on the PC).

With a quick Google search, standard RS-232 cables can be readily purchased thru Amazon and other online sites. For a Serial connection to a PC, the RS-232 cable should be ordered as a DCE to DTE (DB9Female to DB9Male cable, pinned straight-thru, such as pins 1 to 1, 2 to 2, 3 to 3, etc).

For an ethernet/USB connection to the PC, Serial (RS-232) to USB or Ethernet converters are available at sites such as <https://www.perle.com/products/iolan-ds-terminal-server.shtml>. For these converters (an "active" device – not just a "pin adapter") you should specify their device needs to connect to the DB9 RS-232 (DCE device) on the front of the NetClock. A separate DCE (DB9F) to DTE (DB9) serial cable will also likely need to be purchased, and I suspect they should be able to help you with this cable, as well. The serial to Ethernet/Serial to USB converters typically require a specialized driver included with the device be installed on the PC.

Besides also looking online, stores such as Best Buy, Staples or Walmart may also carry serial cables/serial to ethernet converters (years ago, there were several other "PC" stores carrying these types of items , but many of them are now out of business- so online is probably your best bet for finding these two necessary items of the Serial cable and Serial to Ethernet adapter.



---

## CLI (Command Line Interface)

- Our CLI is proprietary. Spectracom created it specifically for our application.
- Type `Helpcli` or `clihelp` for list and descriptions of the available CLI commands.

### Notes:

- 1) Type **Q** to exit help.
- 2) Typing **help cli** or **cli help** (two words instead of one) will respond with “**permission denied**”
- 3) Commands and API calls are cap letter sensitive. Typing any character in the wrong case will cause the command to respond with “**command not found**”.

### Hint: to highlight desired letters or words

- 1) Press the “/” key.
- 2) Type the letters or word to highlight and press enter.

---

## “vi” text file viewer/editor

- Refer to: <https://www.cs.colostate.edu/helpdocs/vi.html>

**Example to edit a file:** Type **vi /etc/sysconfig/network-scripts/ifcfg-eth0**

### To exit vi:

**First press** *shift* + *colon* (: ) to move to the bottom of the file. Then either...

**To save and exit** type **x** <enter> after the colon

**To exit without save (quit)** type **q!** <enter> after the colon

Press *shift* and Type **visual** to edit the file again.

---

## GNU Bash

- NetClocks and SecureSyncs have GNU Bash installed
- The CLI command to obtain the Bash version is: **bash -version** (“dash, dash” before “version”).

---

## Alternate interface to using the limited CLI commands

- Refer to the REST API section of this doc: [\\*\\*\\*\\*secure REST API](#)

---

## \*\*Security with the CLI interface (Ability to connect out using FTP, SCP/SFTP, etc)

Q. We recently purchased two SecureSync NTP appliances. How locked down is the default user account when they log into the cli? (The product appears to be running on Linux.)

**A. From Sam Otto (11 Jul 2013)** The user cannot change configuration files or run most executables. Users must use Spectracom Web UI or CLI commands to configure the system.

To prevent any modifications from the CLI both the Telnet Service and SSH Service can be disabled via Network Services / Network Setup / Services and submitting, refer to the following Picture.



### Security concerns with the Model 1204-06 Option Card installed

- Due to security concerns across Ethernet ports, version 5.1.2 disabled user-level permissions from being able to perform services such as telnet, ssh., FTP and sftp/scp from the command line interface.
- Can still SCP into the SecureSync. This change prevents scp'ing out from the box.
- Can still ping out from within the SecureSync.
- Refer to Salesforce case 13444 and Mantis 2757 for an SCP issue this changed ended up causing

### Trying to FTP from the CLI

```
admin@Spectracom ~ $ ftp spadmin@10.10.201.1
bash: ftp: command not found
```

### Trying to sftp from the CLI

```
admin@Spectracom ~ $ sftp spadmin@10.10.201.1
bash: /usr/bin/sftp: Permission denied
```

**Email from Dave Sohn (4 March 2014)** We have removed local user access to these to prevent security vulnerabilities allowing a user to login from one network and potentially have these accesses to the additional networks that may be connected to the SecureSync. They can still scp to/from the unit, but they need to run it from another machine.

### “su” command to switch users (such as su spfactory) (for internal use only)

- To switch from **spadmin** to **spfactory**, type: **su spfactory** <enter>. Then type the spfactory password
  - Refer to: <https://www.tecmint.com/su-vs-sudo-and-how-to-configure-sudo-in-linux/>
- To switch from **spfactory** back to **spadmin**, type: **su - spadmin** <enter> (with a space before and after the hyphen), Then type the spadmin password
  - Refer to: <https://www.tecmint.com/difference-between-su-and-su-commands-in-linux/>

## Available CLI calls (API calls)

### \*\*\*Troubleshooting issues with CLI commands

#### A) “Error while loading shared libraries” (displayed via RS-232 console connection)

Refer to Salesforce Case 178124 (Nov 2018)

1. LCD display was blank and didn't have access to the web UI, and can't eveping the device.
2. Unit reported as being recently powered-down to relocate it, when issues were observed
3. Error was being displayed on RS-232 console port (not thru ethernet, since ethernet was not communicating)
4. Keith suspects this was due to an older CF card being insalled (which wasn't full, but was likey at least partially corrupt)

```
Login incorrect
Spectracom login: spadmin
Password:
Spectracom SecureSync Version 5.7.1
spadmin@Spectracom ~ $ dhcp4get
dhcp4get: error while loading shared libraries: libsqlite3.so.0: cannot open sha
red object file: Input/output error
spadmin@Spectracom ~ $ hostget
hostget: error while loading shared libraries: libsqlite3.so.0: cannot open shar
ed object file: Input/output error
spadmin@Spectracom ~ $ ip4get
ip4get: error while loading shared libraries: libsqlite3.so.0: cannot open share
d object file: Input/output error
spadmin@Spectracom ~ $
```

All CLI commands respond with **-bash: xxx: command not found** (where “xxx” is the CLI command)

#### Examples

```
spadmin@velasync:~$ helpcli
-bash: helpcli: command not found
```

```
spadmin@velasync:~$ version
-bash: version: command not found
```

```
spadmin@velasync:~$ net
-bash: net: command not found
```

```
spadmin@velasync:~$ ip4get
-bash: ip4get: command not found
```

#### Troubleshooting:

- The correct path is shown in the screenshot below

Can you please send us the response output from the following command: **“echo \$PATH”** (as shown in the example screenshot below):

```
spadmin@Spectracom ~ $ echo $PATH
/usr/cli:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/i686-
pc-linux-gnu/gcc-bin/7.3.0:/usr/i686-pc-linux-gnu/x86_64-pc-linux-gnu/gcc-bin/7.
3.0:/usr/local/bin:/usr/bin:/bin:/opt/bin
spadmin@Spectracom ~ $
```

Try running **“source /etc/profile”** (as shown below):

```
spadmin@Spectracom ~ $ source /etc/profile
spadmin@Spectracom ~ $
```

**Desire to perform more than one CLI command with a single response**

- Separate multiple commands with a semi-colon (“;”) to have just one response.

```
spadmin@Custservice ~ $ dateget; timeget
12 DEC 2015
12:26:00
spadmin@Custservice ~ $
```

**A) “Documented” CLI calls**

- Type **helpcli** for a list of call, descriptions and syntaxes (shift and “q” to exit out)

```
spadmin@Spectracom:~
localget          Display the name of the local clock that is
                  applied to the front panel. Local clocks can
                  only be defined via the Web Browser
                  interface.
localset <clock name> Set the name of the local clock that is
                  applied to the front panel. Local clocks
                  can only be defined via the Web Browser
                  interface.
locallist         Display the list of local clocks that have
                  been defined.
scaleget         Display the timescale of the system clock
scaleset <scale> Set the timescale of the system clock.
                  scale=0 (UTC), 1 (TAI), 2 (GPS)
tfomget          Display the time figure of merit (TFOM) of the
                  system clock to the reference.
oscket           Display the installed system oscillator.

Global Network Commands:
-----
net [info]       The global network commands set or display
                  non-IPv4/6-specific network information.
                  Display a summary of all network configuration
                  items. If an interface is specified, it will
```

- Type **“list”** or help in the home/spectracom directory to display a list of all available CLI calls

```
spfactory@CustService176 /home/spectracom $ list
agns          dns4get  halt      localist  radius    rt6del    sysupgrade
clean         dns4set  helpcli   localset  reboot    rt6get    testevent
cleanhalt    doyget   hostget   model     reftable  saveconf  tfomget
clearlogs    doyset   hostset   net       release4  saveelog  timeget
clearstats   gpsdop   hotstart  net4      release6  scaleget  timeset
clihelp.txt  gpsinfo  ip4get    net6      renew4    scaleset  unrestricted
cliwrapper   gpsloc   ip4set    netnum    renew6    servget   version
dateget      gpsmdl   ip6add    options  resetpw   services  yearget
dateset      gpsreset ip6del    oscget    routes4   servset   yearset
defcert      gpsstat ip6get    portget   routes6   slaacget  zeroize
dhcp4get     gw4get   licenses  portset   rt4add    slaacset
dhcp4set     gw4set   list      portstate rt4del    stateset
dhcp6get     gw6get   loadconf  ppsctrl  rt4get    status
dhcp6set     gw6set   localget  priorset  rt6add    syncstate
```

- The entire list of documented CLI calls is provided in Chapter 5 of the SecureSync manual
  - **Online SecureSync manual at:** [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=cli%20interface](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=cli%20interface)
  - **Shortcut to SecureSync manual (1200-5000-0050) in Arena:** [https://app.bom.com/items/detail-attach?item\\_id=1203165562&version\\_id=10381283008](https://app.bom.com/items/detail-attach?item_id=1203165562&version_id=10381283008)

**Remember:** All commands and API calls are capital letter sensitive. Typing any character in the wrong case will cause the command to respond with “command not found”.

---

## B) “Undocumented”/unsupported CLI calls (calls associated with the TSync boards)

- Refer to the cheat sheet Tim Tetreault created (API for KTS): [..\..\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\CLI -API calls](#)
- Undocumented calls allow “gets” but not “sets” (not available to use for configuration, for example. But can be used to obtain data/settings).

**Remember:** All commands and API calls are capital letter sensitive. Typing any character in the wrong case will cause the command to respond with “command not found”.

The SecureSync’s web browser needs to perform “Get” and “Set” API calls to KTS, in order to show or change information in the system. All of these API calls exist in the background and the “**Get**” calls are available to users, via the CLI interface (the **Set** commands require root account permissions to perform and therefore are not available for customer use).

Note that the Get API calls are “not supported”, but customers can be informed of them and can use them if they wish.

(9/21/12) As of at least 5.8.2 and below, users can only access the “**get**” API calls. They do not have permission to access the “**set**” API calls.

### Unsupported CLI commands (such as FTP/SCP/SFTP etc) due to potential Security concerns

- Due to potential security concerns across Ethernet ports, version 5.1.2 disabled user-level permissions from being able to perform services such as telnet, ssh., FTP and sftp/scp from the command line interface.
- Can still SCP into the SecureSync. This change prevents scp’ing out from the box.
- Can still ping out from within the SecureSync.
- Refer to Salesforce case 13444 and Mantis 2757 for an SCP issue this changed ended up causing

#### Example trying to FTP from the CLI

```
admin@Spectracom ~ $ ftp spadmin@10.10.201.1
bash: ftp: command not found
```

#### Example trying to sftp from the CLI

```
admin@Spectracom ~ $ sftp spadmin@10.10.201.1
bash: /usr/bin/sftp: Permission denied
```

**Email from Dave Sohn (4 March 2014)** We have removed local user access to these to prevent security vulnerabilities allowing a user to login from one network and potentially have these accesses to the additional networks that may be connected to the SecureSync. They can still scp to/from the unit, but they need to run it from another machine.

---

## Display lists of available SecureSync CLI Commands and “Get” API calls

### A) To display a list of ALL available Commands and “Get” API calls

To see a list of all available API calls and available CLI commands, at the CLI command line, hit the TAB key two times. Type a letter “Y” at the prompt that is displayed. ALL available SecureSync commands and KTS **Get** API calls that users can use will be listed. Hit any key to proceed to the next page of listed commands.

**Note**” This does not list any “Set” API calls. Set API calls are not permissible via the SPAdmin or user accounts. Only root has permissions to perform Set calls.

**Example:** at the command prompt, press the TAB key two times to see all of available commands:

**Note:** If no response is shown after hitting the TAB key twice, this is likely due to one or more letters for the call being typed in the wrong case (upper or lower). Re-enter the command using the correct case for each letter.

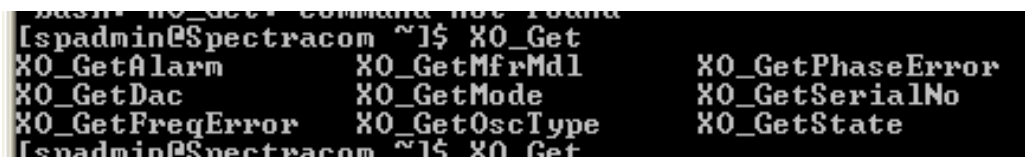
---

### B) To display a list of all commands and Get calls for a particular function (such as all available IRIG gets)

To see a list of all available “Get” calls for a particular function, at the command line, **type the first two characters of the call, followed by the underscore symbol, followed by the word “Get”**. Then, hit the TAB key two times. This will show only the particular API Get calls of that type of call.

**Note**” This does not list any “Set” API calls. Set API calls are not permissible via the SPAdmin or user accounts. Only root can perform set calls.

**Example:** Type “**XO\_Get**” and then press the **TAB** key three times to see all of available XO\_Get type commands:



```
[spadmin@Spectracom ~] $ XO_Get
XO_GetAlarm      XO_GetMfrMdl      XO_GetPhaseError
XO_GetDac        XO_GetMode        XO_GetSerialNo
XO_GetFreqError  XO_GetOscType     XO_GetState
[spadmin@Spectracom ~] $ XO_Get
```

**Note:** If no response is shown after hitting the TAB key twice, this is likely due to one or more letters for the call being typed in the wrong case (upper or lower). Re-enter the command using the correct case for each letter.

---

## \*Specific available CLI commands/API calls/ functions

**exit** to logout

**Note:** The Device ID value for each call (the first number entered after each command) should always be 0 (such as IR\_GetMode 0).

### CLI Commands which no are longer available

#### Mgmt (mgmtget/mgmtset)

**Email from Keith to Mark Day (23 May 13)** I JUST recalled, **mgmt** was a planned command to be able to manage Ethernet ports, but it was then decided not to be used. So it has since been removed in a newer version of software. There is no functionality assigned to it, in earlier versions of software.

**Note:** Refer to Mantis case 1423 (the two “mgmt” commands were removed from the CLI and front panel LCD in Archive version 4.5.0).

Refer to the following section for more information about Management control: [\\*\\*VLANs/Network](#)

## System status commands

Obtain the currently selected Time and PPS references (**SS\_GetRef 0**)

**SS\_GetRef 0** Gets the currently selected time and 1PPS reference.

```
bash: ss_getref: command not found
spadmin@Spectracom ~ $ SS_GetRef 0

Current Active Reference:
Time: gps0
1PPS: gps0
```

## Status

- Reports selected references, NTP Stratum, Osc status, TFOM and MaxTFOM)

```
spadmin@Spectracom ~ $ status
REF:T=ptp0 P=ptp0
NTP:Strat=16 Sync=N
OSC:OCXO (Trk/Lock)
TFOM=10 MaxTFOM=15
spadmin@Spectracom ~ $ █
```

Example '**Status**' command (with NTP Service set to Disabled)

"NTP: Strat=?? Sync=?"=

```
spadmin@Spectracom ~ $ status
REF:T=gps0 P=gps0
NTP:Strat=?? Sync=?
OSC:OCXO (Trk/Lock)
TFOM=2 MaxTFOM=15
spadmin@Spectracom ~ $ █
```

**Email from Keith** (The **status** command is the best CLI command to observe, and to also assume, normal operation of the SecureSync. The NTP status reporting Stratum 1 (or Stratum 2) means the SecureSync is synced to a reference such as GPS (or NTP from another NTP server). Therefore, NTP and PTP are in a state that their associated Slaves can use for their synchronization.

If instead, NTP is Stratum 16, this means there is a problem with the SecureSync's synchronization to its inputs, or there is a problem associated with NTP itself.

Add an additional check for the state of the Fault LED (summary of both Minor/Major alarm states)

Where (note the Power LED is only one color, while Fault/Sync can be bi-color, requiring two controllers each)

Fault LED = LED 0 + LED 1 (**EC\_GetState 0 0 + EC\_GetState 0 1**) ??

Sync LED = LED 2 + LED 2/4 (**EC\_GetState 0 2 + EC\_GetState 0 4**) ??

Power LED = Just LED 5 (**EC\_GetState 0 2 + EC\_GetState 0 4**) ??

In sync Holdover (binking green/red) no sync

|         |       |     |
|---------|-------|-----|
| 0 blink | blink | on  |
| 1 blink | blink | off |
| 2= off  | on    | on  |
| 3 = on  | on    | off |
| 4 off   | off   | off |
| 5       | on    | on  |

- **Fault LED: EC\_GetState 0 0 + EC\_GetState 0 1** (if Fault reports “ON” or “Blinking”, the Minor and/or Major Alarms are active): Blinking/Blinking indicates GPS antenn Problem alarm is asserted???

#### To read individual status indicators

- Sync Status = **SS\_GetSync 0**
- Holdover = **SS\_GetHoldover 0**
- Freerun status = **SS\_GetFreeRun 0**

#### To read the current Alarm status (determine if each individual Alarm is active or inactive)

To read an alarm status, type: **LS\_GetAlarm 0 x** (where x is one of the following values)

- 0 = **Sync** alarm
- 1 = **Holdover** alarm
- 2 = **Frequency Error** alarm
- 3 = **Freerun** alarm
- 4 = **Software error** alarm
- 5 = **1PPS Specification** alarm
- 6 = **Refernce Change** alarm
- 7 = **Hardware error** alarm
- 8 = N/A (there are currently only 7 alarms )

#### **healthcheck.sh** CLI command to check the CF card health

- Believe this this command is available in **v5.8.5 and above**.
- Type: **healthcheck.sh**<enter>

```

Spectracom 166826896 0100 166826896 0100
spadmin@Spectracom ~ $ healthcheck.sh
Nov 08 21:50:43 Spectracom Spectracom: [health] Disk Health OK - No maintenance
required (166826896)
spadmin@Spectracom ~ $ █

```

**Per Ron Dries (8 Nov 2019)** “I found out a customer can issue the command “**healthcheck.sh**” from the cli and it will return the status.”

**Email from Dave L:** There is a CLI command that will check the disc health status; **Healthcheck.sh**  
If your health check reports 3 months or less remaining you should definitely replace the CF card. This is the minimum we recommend for a good firmware update.

**Status update (per Keith 28 April 2023)** I tried this command on the v5.9.6 beta software and it didn’t respond correctly. Not sure if this was due to the convergence build (just affecting the beta) or this command may have



stopped working in a previous version (possibly due to the Write counts now being stored in the sqlite database perhaps??)

If a Western Digital (original) CF card happens to be installed

\$ **healthcheck.sh**

Jun 09 14:38:35 slcicntp02 slcicntp02: [health] Failed to determine health of disk - WD CF Card Detected (4)

- Refer to, in this same document “(Western Digital - WD) CF card happens to be installed”

---

### **manifest: CLI command to display entire manifest.log (v5.7.1 and above only)**

- Command added in version 5.7.1
- Type: **manifest**

```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.7.1
spadmin@Spectracom ~ $ manifest
#####
                        Tue Oct 10 14:46:50 UTC 2017
#####
```

**Note:** For more info on the manifest log, refer to (in this document): [manifest.log file /manifest.config file](#)

**Email from Dave L (10 Oct 17)** Also, starting on the version 5.7.0 firmware there is a new CLI command “**manifest**” you can use to identify the exact Option cards installed on the system. In earlier versions the “options” command would identify the cards but the descriptions were rather generic so the exact model of the options cards was a little vague.

---

### **CLI command for KTS initialization test results (IN\_GetStatus 0)**

- Can find KTS related problems such as an issue with an Option Card at boot-up.
- This command is available to customers in the spadmin account.

**Email from Paul Myers (7 Jun 16):** Can you have the customer run “**IN\_GetStatus 0**” on the command line and look for any initialization failures?

This command prints all the initialized drivers, services and components. If something failed in startup it would show here. (Note the screenshot below is only a partial list)

```
spfactory@CustService176 /home/spectracom $ IN_GetStatus 0

Module | Result
-----|-----
Component Interface | PASS
IRQ Driver | PASS
Watchdog Driver | PASS
Reset Driver | PASS
Timer Driver | PASS
Internal Flash Driver | PASS
External Flash Driver | PASS
Control Status Driver | PASS
Discovery Driver | PASS
Configuration Driver | PASS
SPI Driver | PASS
EEPROM Driver | PASS
Persistent Data Service | PASS
```

## Examples of CLI commands for particular situations:

- 1) Commands regarding the Ethernet ports: Refer to: [CLI Commands for the Ethernet ports](#)
- 2) Apache Web browser no longer accessible, but can still ping, telnet etc. Refer to “free” or “free mem” commands below.
- 3) Available CLI commands for network troubleshooting within SecureSync

---

**Note (Update to the info below)** This info appears to have changed with the Gentoo version 5.0.0 and above release. I don't believe these tools were added in with 5.0.0 and above.

Starting in SecureSync software version 4.8.0, customers will be able to troubleshoot network issues from within SecureSync (instead of just external to the SecureSync). There are several tools being added to provide standard Linux commands for troubleshooting the network traffic. These commands are only available in the CLI port (not on the web browser) and are intended for experienced users only.

### The added commands are:

Ping, ifconfig, arp, rarp, route, netstat, domainname, dig, host, nslookup, traceroute

**For these commands, refer to:** \*\*Network troubleshooting from within SecureSync (ping, arp, traceroute, etc)

---

### rm <filename>:

Deleting/removing a file (such as an upgrade bundle) where permissions allow:

**rm <filename>** <enter>

- To check for any previous updatexxx.tar.gz bundles via CLI, type **ls -l** <enter> (in the home/spectracom directory)
- To delete an update bundle type **rm <filename>** <enter> (for example: **>rm update594.tar.gz** <enter>
  - **spadmin** account does not have permission to delete “.tar.gz” files uploaded via the browser.
  - **-bash: syntax error near unexpected token `('**: To delete a “duplicate” update bundle file (a file name having a number inside of parentheses, such as “**update594(1).tar.gz**”), don't just type the file name verbatim. This will result in “**-bash: syntax error near unexpected token `('**” and the file not being deleted.

```
spadmin@Securesync12 ~ $ rm update595(1).tar.gz
-bash: syntax error near unexpected token `('
spadmin@Securesync12 ~ $ -bash: syntax error near unexpected token `('
> ls
```

- Instead, either put the file name in quotes at the beginning/end, or type “**rm u**” and then press tab. This will auto-populate the file name and also add a couple of “/” characters, as well. Then, the rm command can be successfully performed.

## **\*\*CLI commands enable/disable, display, configure the Ethernet ports (DNS, DHCP, IP address, Subnet mask, Static routes)**

### **Enable/Disable network interfaces via CLI commands (portstate/portset commands)**

**Note:** Since the ports can't be enabled via the keypad in versions prior to v5.5.1, they can only be enabled via either CLI command or via the web browser using eth0

- **For more info on enabling ports via keypad or via the browser, refer to (in this doc):** [\\*\\*Desire to Enable/Disable the Gigabit interfaces \(eth1, eth2 and/or eth3\)](#)

#### **Port state**

- Display the port state of all Ethernet ports (port up, port down, cable unplugged)

#### **portstate command**

**Note:** To obtain port state for SNMP instead of CLI, refer to the “**ifOperStatus**” SNMP object in the SNMP section of this document.

- Displays status of all installed Ethernet ports, including Eth0.

```
spadmin@Spectracom ~ $ portstate
eth0=Up
eth1=Unplugged
eth2=Unplugged
eth3=Unplugged
spadmin@Spectracom ~ $
```

#### **portset command**

- This command was implemented starting with the new web browser design in Archive version 5.1.2 (not available with earlier versions)
- The CLI command: **portset x on** enables the interface number specified by the “x”.
- The CLI command: **portset x off** disable the interface number specified by the “x”
- CLI command to retrieve current port state: **portget x** <enter>

## Enable/Disable link negotiation and ability to hard-set port settings (v5.7.3/5.8.0 and above only)

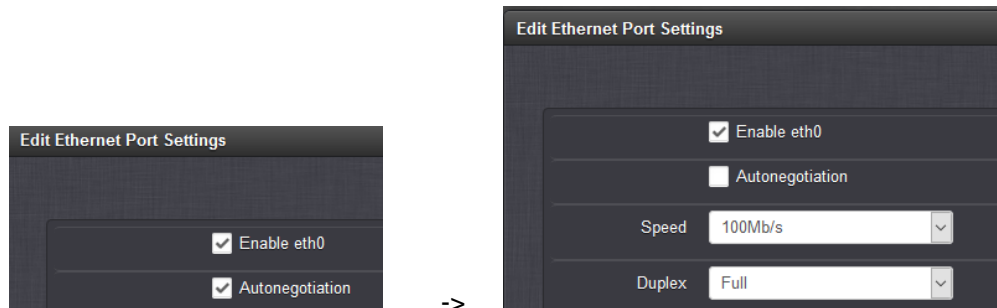
- **Update v5.7.3** (versions 5.8.0/5.8.1 were the next subsequent general release after limited release 5.7.3) added capability to enable/disable link auto-negotiation and set individual network port speed/duplex settings of ethernet interfaces eth0 thru eth3.

➤ Refer to online SecureSync user guide at:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/NCSS\\_Netw\\_Ports.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_Netw_Ports.htm)

### A) Via web browser

1. Navigate to the *Management* -> *Network Setup* page.
2. Unselect the “Autonegotiation” checkbox (selected on all interfaces by factory default)



3. Configure desired speed and duplex
4. Press Submit

### B) Via CLI interface

### C) **speedget** and **speedset** commands (v5.7.3/5.8.0 and above only)

- One of the new features in the next firmware release version 5.8.0 is the ability to control the port settings through the **speedset** and **speedget** CLI commands.

```
spadmin@Spectracom ~ $ speedget
eth0=autoneg on (100Mb/s Full)
eth1=autoneg on (Unknown! Unknown!)
eth2=autoneg on (Unknown! Unknown!)
eth3=autoneg on (Unknown! Unknown!)
spadmin@Spectracom ~ $ speedset
Invalid arguments
Usage: speedset <intfc> <autoneg> (<speed> <duplex>)
  intfc: 0=eth0, 1=eth1, etc.
  autoneg: on|off (provide speed/duplex if autoneg off)
  speed: 10|100|1000
  duplex: full|half
spadmin@Spectracom ~ $
```

## DNS servers (Primary and Secondary DNS servers) (“resolv.conf” file)/LLMNR

- /etc/resolv.conf file stores all DNS server addresses (for all interfaces)

### *resolv.conf file with only one interface configured for DNS*

```
[admin@fsm171 etc]$ cat resolv.conf
nameserver 10.1.1.20
nameserver 10.1.1.31
[admin@fsm171 etc]$
```

### *resolv.conf file with two different interfaces (eth0 and eth1) configured for different DNS servers*

```
spadmin@Spectracom /etc $ cat resolv.conf
# Generated by resolvconf
search domain201 int.orioia.com
nameserver 10.1.1.28
nameserver 10.1.1.29
nameserver 10.1.1.28
nameserver 10.1.1.29
spadmin@Spectracom /etc $
```

DNS servers for eth0

DNS servers for eth1

### *resolv.conf file with two different interfaces (eth0 and eth1) configured for the same two DNS servers*

```
nameserver 10.1.1.29
spadmin@Spectracom /etc $ cat resolv.conf
# Generated by resolvconf
search domain201
nameserver 10.1.1.28
nameserver 10.1.1.29
spadmin@Spectracom /etc $
```

DNS servers for both eth0 and eth1

- Users do not have permission to edit resolv.conf file directly.
- The two DNS Server fields are only displayed in the browser if DHCP is disabled (they are hidden when DHCP is enabled)
- DNS settings should be automatically configured if the port is configured as DHCP enabled
- Manual configuration if DHCP is disabled on that Ethernet interface
- For detailed info on the etc/resolv.conf file, refer to <http://man7.org/linux/man-pages/man5/resolv.conf.5.html>

## CLI commands to Display/Retrieve/Set DNS server settings for each Ethernet interface

- The CLI command: **dns4get x** retrieves the DNS setting (for the port specified by the “x”).
- The CLI command: **dns4set x <primary dns> <secondary dns>** configures the DNS setting for he Ethernet interface port number specified by the “x”. (note the secondard dns address is optional/not required)

## Example journal.log entries associated with DNS

### *Adding two new DNS servers for eth1 via the browser*

Oct 19 14:37:42 Spectracom Spectracom: [webui] set DNS for eth1 to 10.1.1.28.  
Oct 19 14:37:42 Spectracom Spectracom: [webui] set DNS for eth1 to 10.1.1.29.

## The Link-Local Multicast Name Resolution (LLMNR)

- Refer to Salesforce Case 301047
- refer to [https://en.wikipedia.org/wiki/Link-Local\\_Multicast\\_Name\\_Resolution#:~:text=The%20Link%2DLocal%20Multicast%20Name,on%20the%20same%20local%20link](https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution#:~:text=The%20Link%2DLocal%20Multicast%20Name,on%20the%20same%20local%20link)

“The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.”

## Display/retrieve network settings (IP address, subnet mask)

**net** <enter> shows all network settings for all ports

```
spadmin@Spectracom ~ $ net
Hostname: Spectracom
Main IPv4 default gateway (eth0): 10.2.1.1
Main IPv6 default gateway: None

eth0
MAC=00:d0:c9:ba:eb:c9
10.2.100.176/16 S
DHCPv4 (eth0)=Disabled
DG4=10.2.1.1
DNS1:10.1.1.20
INET6 fe80::2d0:c9ff:feba:ebc9/64
DHCPv6 (eth0)=Disabled

eth1 (Unplugged)
MAC=00:0c:ec:05:04:4e
10.10.202.1/16 S
DHCPv4 (eth1)=Disabled
DG4=10.10.202.254
DNS1:10.8.8.1
DHCPv6 (eth1)=Disabled

eth2
MAC=00:0c:ec:04:04:4e
10.2.100.20/16 D
DHCPv4 (eth2)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.26
DNS2:10.1.1.27
INET6 fe80::20c:ecff:fe04:44e/64
DHCPv6 (eth2)=Disabled

eth3 (Disabled)
MAC=00:0c:ec:06:04:4e
0.0.0.0/0 D
DHCPv4 (eth3)=Enabled
DG4=0.0.0.0
DHCPv6 (eth3)=Disabled
spadmin@Spectracom ~ $
```

## Subnet mask conversion table for quick-reference

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

Table 2-3: Subnet mask conversion

**net show** and **net4** commands (net4 is equivalent to net show command in earlier Models)

## Displays All IPv4 settings for all Ethernet port

- The command: **net4** displays or gets the network settings/MAC addresses for each of the network ports.
- IPv4 settings only (no IPv6 settings)

```
Spectracom NetClock 9483 Version 5.0.0
spadmin@Spectracom ~$ net4
Hostname: Spectracom
Main IPv4 default gateway (eth0): 10.2

eth0
00:d0:c9:c9:04:6b
10.2.100.171/16 S
DHCPv4(eth0)=Disabled
DG4=10.2.1.1

eth1
00:0c:ec:05:02:e2
10.2.100.82/16 D
DHCPv4(eth1)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31

eth2
00:0c:ec:04:02:e2
0.0.0.0/0 S
DHCPv4(eth2)=Disabled
DG4=0.0.0.0

eth3
00:0c:ec:06:02:e2
0.0.0.0/0 D
DHCPv4(eth3)=Enabled
DG4=0.0.0.0
spadmin@Spectracom ~$
```

## Display IPv6 settings only (no IPv4 settings)

- The command: **net6** displays the network settings/IPv6 addresses for each of the network ports.

```
eth0
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6(eth0)=Disabled

eth1
DHCPv6(eth1)=Disabled

eth2
DHCPv6(eth2)=Disabled

eth3
INET6 fe80::20c:ecff:fe06:2e2/64
DHCPv6(eth3)=Disabled
[spadmin@Spectracom ~]# net6
Spectracom
Main IPv6 default gateway: None
```

## Display Eth0 settings only (Both IPv4 and IPv6 settings)

- **net settings** command displays only Eth0's IPv4 and IPv6 network port configurations
- Shows no info on Eth1, Eth2, Eth3

```
[spadmin@Spectracom ~]# net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None

eth0
MAC=00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4(eth0)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6(eth0)=Disabled
[spadmin@Spectracom ~]# net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None
```

---

## DHCP (V4 and V6)

### A) DHCP4

- Get all current DHCP settings: **dhcp4get**
- Get current DHCP setting for one particular port: **dhcp4get <interface>** (such as **dhcp4get 0**)
- Enable DHCP setting: **dhcp4set <interface> on** (such as **dhcp4set 0 on**)
- Disable DHCP setting: **dhcp4set <interface> off** (such as **dhcp4set 0 off**)

### B) DHCP6

- To set a static IPv6 address, you must first turn off DHCP for IPv6
  - **dhcp6get** Display whether DHCP is enabled. Get all current DHCP settings
  - **dhcp6set 1 off** turning off dhcp on port eth1.
- Get current DHCP setting for one particular port: **dhcp4get <interface>** (such as **dhcp4get 0**)
- Enable DHCP setting: **dhcp4set <interface> on** (such as **dhcp4set 0 on**)
- Disable DHCP setting: **dhcp4set <interface> off** (such as **dhcp4set 0 off**)
- **dhcp6get** – Display whether DHCP is enabled.
- **dhcp6set 1 off** – turning off dhcp on port eth1.

---

## \*\*\*\*Assigning network settings

- **IP4get <interface>** (such as **IP4get 0**)
- **IP4set <interface> <address> <mask>** (such as **IP4set 0 10.10.200.1 255.255.255.0**)

### IP Address

- Get current IPv4 address (can't display all at once): **IP4get <interface>** (such as **IP4get 0**)
- Set IP address: **IP4set <interface> <address> <mask>** (such as **IP4set 0 10.10.200.1 255.255.255.0**)

---

## Gateway addresses (Main default gateway as well as the gateway address for each port)

### A) IPv4 gateway

#### Get current gateway address:

- **gw4get** Displays gateway address for all Ethernet ports.
- **gw4get <interface>** (such as **gw4get 0**) for one particular gateway address
- **Note** <interface> is 0, 1, 2, 3 or m for main default gateway.

Enable and set gateway address: **gw4set <interface> <'gateway address>** (example **gw4set m 10 10.10.200.1**)

#### Get (read) gateway



- CLI command to read which port is the main default gateway: **gw4get m** <enter> (where m is for main)
- CLI command to read the gateway address for a particular Ethernet port (eth2 for example): **gw4get 2** <enter>

### Set gateway

- CLI command to **set** which port is the main default gateway: **gw4set m x y** <enter> (where **m** is for “main”, **x** is the gateway address and **y** is the port number.

Example to make the default port 2: **gw4set m 10.2.1.1 2** <enter>

```

[spadmin@Spectracom ~]$ net4
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1

eth0
00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4(eth0)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31

eth1
00:0c:ec:05:02:e2
0.0.0.0/0 D
DHCPv4(eth1)=Enabled
DG4=0.0.0.0
DNS1:10.1.1.20
DNS2:10.1.1.31

eth2
00:0c:ec:04:02:e2
0.0.0.0/0 D
DHCPv4(eth2)=Enabled
DG4=0.0.0.0

eth3
00:0c:ec:06:02:e2
10.10.204.1/16 S
DHCPv4(eth3)=Disabled
DG4=10.10.204.254
[spadmin@Spectracom ~]$

```

### B) IPv6 gateway address

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

- Refer also to: [\\*\\*Interface gateway addresses \(IPv4/IPv6\)](#)

**gw6set 1 xxx.xxx.xxx.xxx** – sets the IPv6 gateway address

Usage: gw6set <on|off> [addr]  
 addr: IPv6 address, ie. fe80::230:64ff:fe04:3ef8

**Email from Ron D (19 Sep 17)** about the IPv6 link-local address, in software version 5.7.1 the functionality to set the IPv6 gateway to the link-local address was only added to the CLI.

To set the IPv6 gateway to the link-local address the gw6set command needs to be used.  
 The command usage is: “gw6set <on|off> [addr] <intfc>”

Where “addr” would be the link-local address and “intfc” is the Ethernet interface to apply it to. So an example of the command to set the link-local address as the gateway for eth0 would be “gw6set on fe80:: 0”.

- ip6add 1 (IP xxx.xxx.xxx.xx) (subnet address xxx.xxx.xxx.xxx) (gateway address xxx.xxx.xxx.xxx)

- o ip6add 1 **xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx** (adds IPv6 IP address, subnet and gateway for eth1)

**Issues with configuring IPv6 gateway address (such as not being able to use a link-local address)**

- Refer to: [\\*\\*Interface gateway addresses \(IPv4/IPv6\)](#)

**Ifconfig / ip addr**

- just type **“ifconfig”** or **“ip addr”**

**Function:** allows the operating system to setup network interfaces and allow the user to view information about the configured network interfaces.

**Displays:** all IP addresses, subnet masks, MAC addresses, received/transmitted packets, dropped packets, packet collisions, etc

**Netmask conversion table for quick-reference**

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

Table 2.2: Subnet mask values

**Ifconfig -a** (Shows status of all network ports) (example below just shows a couple of the Ethernet ports)

```
Spectracom NetClock 9483 Version 4.8.8
ispadmin@Spectracom ~$ ifconfig -a
eth0
Link encap:Ethernet HWaddr 00:D0:C9:C9:04:6B
inet addr:10.2.100.3 Bcast:10.2.255.255 Mask:255.255.0.0
inet6 addr: fe80::2d0:c9ff:fe09:46b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4714879 errors:0 dropped:0 overruns:0 frame:0
TX packets:2619897 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:53283302 (507.9 Mb) TX bytes:393514456 (375.2 Mb)
Interrupt:10 Base address:0xec00

eth1
Link encap:Ethernet HWaddr 00:0C:EC:05:02:E2
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:11 Memory:efec0000-efee0000

eth2
Link encap:Ethernet HWaddr 00:0C:EC:04:02:E2
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:7 Memory:efdc0000-efde0000
```

**ifconfig eth0** (Shows only Eth0 status) – same for Eth1, Eth2 or Eth3

```
ispadmin@Spectracom ~$ ifconfig eth0
-bash: ifconfig: command not found
ispadmin@Spectracom ~$ ifconfig eth0
eth0
Link encap:Ethernet HWaddr 00:D0:C9:C9:04:6B
inet addr:10.2.100.3 Bcast:10.2.255.255 Mask:255.255.0.0
inet6 addr: fe80::2d0:c9ff:fe09:46b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:887418 errors:0 dropped:0 overruns:0 frame:0
TX packets:3841 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:75307736 (71.8 Mb) TX bytes:360429 (351.9 Kb)
Interrupt:10 Base address:0xec00
```

## IP addr (IP Address)

```
spadmin@Spectracom ~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: tun10: <NOARP> mtu 1480 qdisc noop state DOWN
    link/rtnl 0.0.0.0 brd 0.0.0.0
3: sit0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
4: ip6tn10: <NOARP> mtu 1452 qdisc noop state DOWN
    link/tunnel6 :: brd ::
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ether 00:d0:c9:c9:04:6b brd ff:ff:ff:ff:ff:ff
    inet 10.2.100.171/16 brd 10.2.255.255 scope global eth0
    inet6 fe80::2d0:ccff:fec9:46b/64 scope link
        valid_lft forever preferred_lft forever
6: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether 00:0c:ec:05:02:e2 brd ff:ff:ff:ff:ff:ff
7: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:ec:04:02:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.251.21.135/16 brd 10.251.255.255 scope global eth2
    inet6 fe80::20c:ecff:fe04:2e2/64 scope link
        valid_lft forever preferred_lft forever
8: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether 00:0c:ec:06:02:e2 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:ecff:fe06:2e2/64 scope link
        valid_lft forever preferred_lft forever
spadmin@Spectracom ~$
```

---

## Configure Static Routes

Refer to "[Static Routes](#)" (Static Routing) in the "Network" section further below in this document

## GPS receiver (GR\_) calls

Refer to the GNSS/GPS info section (in Inputs) of this document

---

## Reading/ manually setting Date and Time (via cli or browser)

**IMPORTANT NOTE: USER/USER** input reference **MUST** be enabled in the reference priority table in order to be able to manually change the date/time via the web browser, CLI interface (such as dateset or doysset) or front panel. If USER/USER is not enabled, the time/date will not be changed.

- Note: If any inputs are present and valid with a higher priority than the user/user reference, the higher priority reference will override the manual set time.

### A) timeget/timeset (System Time)

In addition to the time being displayed in the browser, the SecureSync's UTC time can also be queried using a CLI command (via a telnet or SSH session). The CLI command to read the current time is "**timeget**" as shown below:

#### timeget

```
spadmin@Spectracom ~$ timeget
15:40:27
```

#### timeset

```
Usage: timeset <hh> <mm> <ss>
```

## Desire for timeget command to provide milliseconds resolution

- Refer to Salesforce Case 265275

- Refer to **HW\_GetTime 0** and **CS\_GetTime 0 0** calls further below (partial excerpts directly below). **Note:** Both these calls can be performed by spadadmin account.

The **CS\_GetTime 0 0** KTS call reads the System Date and Time and is also used in the system to update the front panel. **CS\_GetTime 0 1** and **CS\_GetTime 2** also shown below

```
spadmin@Spectracom ~ $ CS_GetTime 0 0
DOY Time:
Year: 2015
DOY: 113
Hr: 14
Min: 56
Sec: 59
Nsec: 460692570
DST State: Standard Time

spadmin@Spectracom ~ $ CS_GetTime 0 1
BCD Time:
Year: 2021
DOY: 148
Hr: 17
Min: 19
Sec: 41
Msec: 476
Usec: 943
DST State: Standard Time

spadmin@Spectracom ~ $ CS_GetTime 0 2
DST State: Standard Time
Sec Time:
Sec: 162222471
Nsec: 209741750
DST State: Standard Time
```

### The **HW\_GetTime 0**

```
spadmin@Spectracom ~ $ HW_GetTime 0
DOY Time:
Year: 2021
DOY: 148
Hr: 17
Min: 09
Sec: 18
Nsec: 329932870
Sync: TRUE
spadmin@Spectracom ~ $ CS_GetTime 0 0
```

OR, Both calls performed at the exact same time

```
spadmin@Spectracom ~ $ HW_GetTime 0; CS_GetTime 0 0
DOY Time:
Year: 2021
DOY: 148
Hr: 17
Min: 09
Sec: 59
Nsec: 703976710
Sync: TRUE

DOY Time:
Year: 2021
DOY: 148
Hr: 17
Min: 09
Sec: 59
Nsec: 731910450
```

## B) dateget/dateset (System Date)

- **dateget** retrieves the System Date
- **dateset** is used to set the System Date

```
spadmin@Spectracom ~ $ dateget
23 APR 2015
spadmin@Spectracom ~ $ dateset
Invalid arguments
Usage: dateset <mm> <dd> <yyyy>
spadmin@Spectracom ~ $
```

### C) Doyset/doyget (System Day of Year)

**doyget** and **doyset**

```
spadmin@Spectracom ~ $ doyget
113
spadmin@Spectracom ~ $ doyset
Invalid arguments
Usage: doyset <doy>
spadmin@Spectracom ~ $
```

### D) System Year

CLI commands to obtain/change the System Year

**yearget**

**yearset xxxx**

```
spadmin@Spectracom ~ $ yearset 2020
spadmin@Spectracom ~ $ yearget
2020
spadmin@Spectracom ~ $
```

### E) Date (Linux OS date and time)

The **date** command reads the Linux OS date and time (not the System Time's date). The proper CLI command to read the current System Date is instead "**date**" as shown above:

```
spadmin@Spectracom ~ $ date
Thu Apr 23 15:02:36 UTC 2015
spadmin@Spectracom ~ $
```

**dateset <mm> <dd> <yyyy>**

### F) **CS\_GetTime 0 0** <enter>

- This KTS call reads the System Date and Time and is also used in the system to update the front panel.

```
spadmin@Spectracom ~ $ CS_GetTime 0 0
DOY Time:
Year: 2015
DOY: 113
Hr: 14
Min: 56
Sec: 59
Nsec: 460692570
DST State: Standard Time
```

(CS\_GetTime 0 1 and CS\_GetTime 0 2 also shown below, for format comparisons)

```
spadmin@Spectracom ~ $ CS_GetTime 0 1
BCD Time:
Year: 2021
DOY: 148
Hr: 17
Min: 19
Sec: 41
Msec: 476
Usec: 943
DST State: Standard Time
spadmin@Spectracom ~ $

spadmin@Spectracom ~ $ CS_GetTime 0 2
DST State: Standard Time
Sec Time:
Sec: 1622222471
Nsec: 209741750
DST State: Standard Time
spadmin@Spectracom ~ $
```

### G) HW\_GetTime 0

```
spadmin@Spectracom ~ $ HW_GetTime 0
DOY Time:
Year: 2021
DOY: 148
Hr: 17
Min: 08
Sec: 31
Nsec: 745369510
Sync: TRUE
```

### H) Obtaining the next scheduled leap second

#### CS\_getLeapSec 0

```
Time Scale Offset for GPS: 17
spadmin@Spectracom ~ $ CS_GetLeapSec 0
Leap Second: +1 sec at 00:00:00 001/2017 UTC
spadmin@Spectracom ~ $
```

### I) Get the offset (in seconds) between GPS time and UTC time

#### CS\_GetTimeScaleOff 0 2 (where the "2" indicates the offset for GPS time scale)

```
spadmin@Spectracom ~ $ CS_GetTimeScaleOff 0 2
Time Scale Offset for GPS: 17
spadmin@Spectracom ~ $
```

---

### passwd: Change the spadmin account password via CLI

- Per the note further below, in at least versions 5.7.0 and below, the rules for passwords being created/changed in the browser are not being applied to passwords being changed via the CLI.
  - **Per JIRA-SSS-259:** See info further below about a post 5.7.0 update intending on the ability to configure the password via CLI being forbidden. Due to the password rules only being available via the browser, this intention is to prevent anyone from using the cli to change a password, with no restrictions on the intended

password.

```
spadmin@Spectracom ~ $ passwd
Changing password for spadmin.
(current) UNIX password: [ ]
```

**Note about the available “Password Security” Rules in the browser (*Management -> Authentication* page)**

- Per Salesforce case 25067, and in at least versions 5.7.0 and below, the Password Security rules that can be custom configured in the browser (such as special characters, min length, expiry, etc) don't currently apply to the passwd command. These available 'rules' ONLY apply when creating/changing passwords via the BROWSER.
  - Reference **JIRA ticket SSS-259** (<https://spectracom.atlassian.net/browse/SSS-259>)
  - For more info on Password Security rules: [“Password Security” \(Available minimum password requirements that can be enforced, if desired\)](#)

**Follow-up status from Engineering/Product Management on this condition**

**Email from Paul Myers (4 Aug 17, referring to a planned change in post v5.7.0) JIRA-SSS-259 is changed to FORBID use of passwd command to change passwords for any users other than spfactory or root.**

**User's must change passwd and passwd rules form Web UI. Change approved by Product Management for SecureSync: David Sohn.**

---

**Model and Unit's Serial Number**

**model**

```
spadmin@setimex1 /usr/cli $ model
SecureSync
Model No: 1200-233
Serial No: 05861
```

**Note:** To change the Model Number, login as **spfactory** and type **modno**

**Software Issue with Model command (“you must be an administrator to invoke the model command”)**

- Refer to Case 217323  
Spectracom SecureSync Version 5.8.6  
mhigashi@clock02-ny5 ~ \$ model  
**You must be an administrator to invoke the model command.**

---

**Oscillator type and Serial Number**

**Type of osc installed**

**Oscget (or XO\_GetOscType 0)**

```
spadmin@setimex1 /usr/cli $ oscget
```

```
Serial No: 1337
spadmin@Spectracom ~ $ oscget
OCXO (5ppb)
spadmin@Spectracom ~ $
```

Rubidium (.1ppb)

Osc Serial Number:

**XO\_GetSerialNo 0**

---

**stateset:** Enable/disable entries already in the Reference Priority table (changes the “State”)

```
spadmin@Spectracom176 ~ $ stateset
Invalid arguments
Usage: stateset <index> <state>
index: 0..15
state: 0=disable, 1=enable
spadmin@Spectracom176 ~ $ █
```

---

**gettemp:** Obtain Oscillator, board and CPU temperature readings via CLI (applicable to versions 5.4.5 and above only)

- Version 5.4.5 added the **gettemp** command to allow reading of temperatures.

```
spadmin@Spectracom ~ $ gettemp
Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ gettemp
Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $ gettemp osc
N/A
spadmin@Spectracom ~ $ gettemp board
74.00 degrees C
spadmin@Spectracom ~ $ gettemp cpu
92.00 degrees C
spadmin@Spectracom ~ $ █
```

---

**Options:** CLI command to list all installed Option Cards

```
spadmin@Spectracom /home/spectracom $ options
1:IRIG 2324:None
2:Gb Eth 5:PPS TTL
3:485 RLY6:GB PTP
spadmin@Spectracom /home/spectracom $ █
```

**Note:** Also in newer firmware version 5.7.1 and higher units, the “**manifest**” command will show all the system information in more detail.

---

**\*\*Version commands (Linux OS and Spectracom software)**

**A) Read the current version of Linux OS**

- SecureSync runs on a Linux OS.

CLI commands to read Linux OS version:

**cat /proc/version**



```
spadmin@Spectracom ~ $ cat /proc/version
Linux version 3.8.13-gentoo (root@localhost) (gcc version 4.6.3 (Gentoo 4.6.3 p1
.13, pie-0.5.2) ) #1 PREEMPT Wed Jul 3 05:07:14 Local time zone must be set--see
z
spadmin@Spectracom ~ $
```

## uname -a

```
spadmin@SpectracomCS176:~
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.7.3
spadmin@SpectracomCS176 ~ $ uname -a
Linux SpectracomCS176 4.4.87-gentoo-r1 #17 Tue Jan 23 16:17:44 UTC 2018 i586 Geo
de(TM) Integrated Processor by AMD PCS AuthenticAMD GNU/Linux
spadmin@SpectracomCS176 ~ $
```

## B) Spectracom software version

Post version 4.4.0 (V4.5.0) software versions have an available version command (“**Version xxx**”) in the CLI to query for the versions of the different modules (SNMP, GPS, Apache, SSH, SSL, etc). (These values not planned to be added to the browser display). Below is a list of specific commands (with a space in between the word “version” and the module name:

**Note:** First letter “version” has to be lower-case.

“**version**” (with nothing after it) reports the Archive and Timing System versions

```
[spadmin@Spectracom ~]$ version
Software      4.8.8
Timing System 2.8.8
Build Time    Dec 6 2012 11:37:03
[spadmin@Spectracom ~]$ free
```

## version SNMP (shown with 4.8.8 installed)

```
NET-SNMP version: 5.6.1
Web: http://www.net-snmp.org/
Email: net-snmp-coders@lists.sourceforge.net
```

## version GPS

```
[spadmin@Spectracom ~]$ version gps
Mfr/Mdl: Trimble Resolution T
GR (0) Rcv Info (66 bytes):
-----
Serial #: 2048 21426123
Date: 7/15/2011
-----
Appl Ver: 1.20
Date: 4/21/2010
-----
Core Ver: 1.26
Date: 4/21/2010
-----
[spadmin@Spectracom ~]$
```

**version web** (not "version apache") (shown with 4.8.8 installed)

```
Server built: Oct 30 2012 18:41:41
[spadmin@Spectracom ~]$ version web
Server version: Apache/2.2.23 (Unix)
Server built: Oct 30 2012 18:41:41
[spadmin@Spectracom ~]$
```

**version SSL** (shown with 4.8.8 installed)

```
Server built: Oct 30 2012 18:41:41
[spadmin@Spectracom ~]$ version ssl
OpenSSL 1.0.1c 10 May 2012
[spadmin@Spectracom ~]$
```

**version SSH** (shown with 4.8.8 installed)

(or **ssh -v**)

```
[spadmin@Spectracom ~]$ version ssh
OpenSSH_6.1p1, OpenSSL 1.0.1c 10 May 2012
[spadmin@Spectracom ~]$
```

**version NTP**

(shown with 5.0.2 installed)

```
spadmin@Spectracom ~/log $ version ntp
ntpq 4.2.6p5@1.2349-o Wed Jul 3 03:37:01 UTC 2013 <1>
spadmin@Spectracom ~/log $
```

(shown with 4.8.8 installed)

```
OpenSSH_6.1p1, OpenSSL 1.0.1c 10 May 2012
[spadmin@Spectracom ~]$ version ntp
ntpq 4.2.0@1.1161-r Tue Nov 27 11:00:23 EST 2012 <1>
[spadmin@Spectracom ~]$
```

---

**defcert or defcert -sha1** (delete the HTTPS certificate)

- The only CLI command associated with certificates is the **defcert** command (to reset the certificate back to default)
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - An example defcer CLI syntax (5.6.0 and above only) is **defcert -sha256**
  - V5.6.0 also changed the default algorithm to **SHA256** for better security (the default in 5.5.1 and below was SHA1) .
  - As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access to IE8 and below

**Email from Keith (20 Jul KW)** One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can't use this newer

cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

---

## GNU Bash

- NetClocks and SecureSyncs have GNU Bash installed
- The CLI command to obtain the Bash version is: **bash -version** (“dash, dash” before “version”).

---

## CLI COMMANDS FOR 1204-3D Sateltes STL receiver (versions 5.6C and above only)

### STR\_GetSubscription 0 0

- Reports end of subscription.

```
Spectracom SecureSync Version 5.6.C  
spadmin@Spectracom ~ $ STR_GetSubscription 0 0
```

```
RESPONSE End of Subscription: 01/06/1980
```

## “STR\_” error messages in System log (Versions 5.8.0 through 5.8.4 only)

### “ERROR in KTSAL\_Get:SPEC\_KTSAL\_EN=true STR\_GetSubscription 0.0 (KTSAL)”

- Refer to JIRA ticket SSS-505 (completed ~11 Feb 2019)
- Refer to SF cases such as 171405
- Fixed in 5.8.5 update (July 2019)
  - *Per update version 5.8.5 release notes* “Fixed a minor issue with errors from the STL front panel status display.”
- Was caused by “**STL INFO**” menu being displayed on front panel (or rotate menus selected) with no 1204-3D/1204-3E STL card installed in the system
- Version 5.8.0 added the STL Info menu in all units, even if 1204-3D/3E is installed. If the unit is downgraded to below 5.8.0, this STL menu is no longer exists - so the issue no longer occurs.
- If STL card isn’t installed, the request by the front panel to display STL data causes an error message to be asserted.

**email from Keith (1 Nov 18)** This “GetSubscription” entry is associated with a purchasable feature we now offer for SecureSyncs, called “STL”. In case you aren’t familiar with it, it’s a satellite signal, similar to GPS, but since these satellites are closer to the earth than the GPS constellation, their signals are stronger. There are other benefits to it, as well.

STL is available with an STL receiver Option Card and a subscription to the service. The version 5.8.0 software update added a new front panel LCD display menu which shows the signal strength of this STL signal. The error message just means that someone was scrolling through the various menu screens, which include the STL menu. But without the STL receiver/option being installed, there was no communications available to report the expected value.

This “errant” entry is expected to be no longer reported if the STL menu is selected, or scrolled thru, via a future software update. There should be no operational concerns if this entry is observed! Thanks again for asking about it, just to be sure it didn’t indicate a problem!!

## Viewing the logs in the web browser

### A) Newer browser

In versions 5.1.2 to at least 5.3.1 (this is expected to be changed in 5.4.0, ~ Jan 2016) the newer (black/charcoal) browser only displays the most current set of entries (the file with no number). This is being changed to allow the newer browser to display all the logs. In the earlier versions, “all” log entries can only be displayed in the classic interface or via a cli connection.

#### Ability to view the logs (log entries) with the CLI interface

- A) Login with **telnet/ssh**
- B) Type **cd log** to change to the log directory
- C) Type **ls** to list all log file names
- D) Type **cat** followed by the name of the log (including the file extension).

#### With versions 5.0.2 or higher installed

```
Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ cd log
spadmin@Spectracom ~/log $ ls
alarms.log  cron.log.2  discstats  mail.log  qual.log  system.log
auth.log   cron.log.3  events.log  ntp.log  rexd.log  timing.log
cron.log   cron.log.4  journal.log ntpstats snmpd.log update.log
cron.log.1 daemon.log  kern.log   osc.log  sys.log  user.log
spadmin@Spectracom ~/log $
```

#### With versions 4.8.9 or prior installed

```
[spadmin@CustomerService log]$ ls
alarms.log  cron.log.4  kern.log.1  osc.log.2  snmpdbg.txt  system.log
auth.log    daemon.log  mail.log    osc.log.3  sys.log      timing.log
cron.log    discstats  ntp.log     osc.log.4  sys.log.1    update.log
cron.log.1  events.log  ntpstats   qual.log   sys.log.2    user.log
cron.log.2  journal.log osc.log     qual.log.1 sys.log.3
cron.log.3  kern.log   osc.log.1  snmpd.log  sys.log.4
[spadmin@CustomerService log]$
```

## Viewing the log bundle file on a linux box or Windows PC

Q What linux command line argument can I use to “untar” the log files so I can read them?

**A Keith's response (12 Jan 17) :** The log bundle is a tar.gz file. You can use “**tar**” in linux to examine the log bundle. Or, you can also use either Winzip or 7-zip in a Windows PC to open the bundle.

## Ability to Save/backup logs via CLI

- Version 4.8.8 (Dec 2012-ECN 3099) Added **savelog** CLI command to handle log backup.
- Versions 4.8.7 and below- not available

#### **savelog** <file name> <enter>

- This command saves the system log bundle to the following directory: /Home/Spectracom/Xfer/Log
- Then the user can manually FTP/SCP the log bundle file from this directory.

#### Note:

- FTP port is port 21
- SCP port is port 22

## Ability to delete the logs via CLI

- Version 5.1.5 introduced the **clearlogs** CLI command

- Can't delete the logs via CLI before version 5.1.5

## Saved log bundle way too small (only ~15kb) when downloaded using browser and only contains HTML code when opened

- Update to bullet directly below (11 Dec 15 KW) it now appears this condition is caused by the log bundle file being too large to download using the web browser. This particular condition was noticed again with another unit and Ron Dries had the customer look at the size of the log file while still in the SecureSync. It was a valid size, even though it was only 15kb when downloaded using the browser. Log bundle was also confirmed fine after extracting it via the CLI (FTP/SFP)

**Email from Ron to Eric Girard (11 Dec 15)** Could you have him check the log bundle on the SecureSync in the /home/spectracom/xfer/log directory?

Check to make sure that the bundle was created around the time that he clicked the save and download logs button, and the file size.

To do this have him issue the following command in the directory: "ls -la" and send us the screenshot, and if the bundle is there have him send us that as well.

I had this happen to me, and what it looked like is we were saving the log bundle on the system but it was too large to download from the web UI.

**Temporary work-around if this condition happens:** After saving/creating the log bundle in the browser (or performing a **savelog** CLI command) manually extract the bundle using FTP or SCP (instead of using the browser to download it). The securesync.log bundle file is located in the following directory:  
/home/spectracom/xfer/log

```
spadmin@spectracom /etc/ntp $ cd /home/spectracom/xfer/log
spadmin@spectracom /home/spectracom/xfer/log $ ls
spadmin@spectracom /home/spectracom/xfer/log $ ls
spadmin@spectracom /home/spectracom/xfer/log $ cd ..
spadmin@spectracom /home/spectracom/xfer $ ls
spadmin@spectracom /home/spectracom/xfer/log $ ls
spadmin@spectracom /home/spectracom/xfer/log $ savelog
Invalid arguments
Usage: savelog <log archive filename>
spadmin@spectracom /home/spectracom/xfer/log $ savelog securesync.log
/home/spectracom/xfer/log/securesync.log
Creating Log Archive at /home/spectracom/xfer/log/securesync.log
tar: Removing leading '/' from member names
kltar: Removing leading '/' from hard link targets
spadmin@spectracom /home/spectracom/xfer/log $ ls
securesync.log
spadmin@spectracom /home/spectracom/xfer/log $
```

- Per Ron and Paul (9 Nov 15) they believe this is a factor of the SecureSync still being in an abnormal state when the logs were bundled.
  - They recommend rebooting the unit and then try saving the logs again.

### Example entries below, when this condition has occurred

```
!DOCTYPE html>
<html>
<head>
  <!-- Always force latest IE rendering engine or request Chrome Frame -->
  <meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />  <!--nocache-->
  <title>
    MEY-MNC02  </title>
  <!--nocache-->
  <link href="/favicon.ico" type="image/x-icon" rel="icon" /><link href="/favicon.ico" type="image/x-icon" rel="shortcut
  icon" /><link rel="stylesheet" type="text/css" href="/css/lafayette.css" /><script type="text/javascript"
  src="/js/lafayette.js"></script><script type="text/javascript" src="/js/helper.js"></script>
  <!--[if lt IE 9]>
  <script type="text/javascript" src="/js/html5shiv.js"></script><script type="text/javascript"
  src="/js/excanvas.js"></script><script type="text/javascript" src="/js/iefix.js"></script><link rel="stylesheet" type="text/css"
```

```

href="/css/iefix.css" /> <![endif-->

<script type="text/javascript" src="/util/dygraph-combined.js"></script>
<meta name="viewport" content="width=device-width, maximum-scale=1, initial-scale=1, user-scalable=0">

</head>
<body>

<div class="container-fluid page-container">
  <!--nocache-->
  <script type="text/javascript">$(document).ready( function() {});</script> <!--/nocache-->
  <div id="banner">
    <div class="row-fluid">
      <div id="bannerTop" class="span12">
        <div class="row-fluid">
          <div id="bannerLogo" class="logo span5 pull-left"></div>
          <div id="bannerDeviceName" class="Devicename span4 pull-right">
            <div class='elem_DeviceName'>
              <span> <a href="/">SecureSync</a> </span>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>

```

---

## Desire to automatically delete the logs on a periodic schedule

Q Can we automate (or setup) log cleaning on the Spectracom GPS-Clock for a predetermined period ?

**A Keith's response:** The short answer is the logs cannot be automatically deleted/cleaned based on a predetermined period. Instead, each log file (such as the Alarms log, Events log, Qualification log, etc) is independently cleared as necessary, based on a defined log file size (the logs are rotated to delete the oldest entries first).

**The longer answer:** When the unit's logs are configured to be stored within the time server (this is the factory default configuration, as configured in the **Management -> Log Configuration** page of the browser. Note most of the logs can be optionally sent to a syslog server and configured not to be stored in time server at all) each individual log file is automatically rotated and cleared, when each file has reached a certain size. After the earliest log entices have been rotated to a fourth log file of a similar name, the oldest entries of that particular log file are deleted.

Besides configuring the logs to not be stored in the server- they can instead just be sent to a remote Syslog server (and the factory default hard-set log rotation in the software) there is no other way to internally automate the logs being deleted on a specified/periodic basis.

However, there is a CLI command that will delete the logs (the logs can be commanded to be cleared/deleted via either the browser or CLI). If desired, they can create a custom script that logs into the CLI interface (telnet or SSH) when desired and then performs the CLI command: clearlogs <enter> (this command is available in software versions 5.2.1 and above).

---

## Testing SNMP traps and email alerts (**testevent** and **sendtrap** commands)

- Refer to (in this document): [\\*\\*Testing/Verifying SNMP/Email alerts are enabled and working inside the SecureSync](#)

## System Start-Up sequence/boot-up and initial effects of Signature Control on outputs

### Special patch modifying start-up sequence of GPS sync (~Jun 2018)

- Reference Salesforce Case 164267
- Refer also to emails/patch located at: [..\..\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates\Previous-debug SecureSync updates\1-patches not changing version\SF Case 164267 startup sequence](#)

**Reported issue:** AS we discussed yesterday we have a customer, **EF Johnson having issues with the Securesync power on sequence. Their Securesyncs with signature control set for “Enabled in Holdover” will continuously output the 10 MHz and 1PPS upon startup. The Securesync will go right into Holdover mode and the outputs remain on, which causes major problems for their radio transmitter when the Securesync syncs to GPS and the timing shifts.**

We discussed writing a script or modifying the config file to allow the system to startup with no references available for sync.

**Another email from Dave L (4 Jun 18)** They have updated to v5.8.0 and their system is continuously powering up and going immediately into Holdover mode. The desired operation is to output only good timing using Signature Control in Sync and Holdover modes after the Securesync has synchronized and stabilized. Having the Securesync go into Holdover mode before the timing is good negatively affects their radio transmitters.

Sometimes it comes up In Holdover right away and other times it comes up Out of Sync and operates as expected. The Securesync is not consistent.

### Start-up Questions/Answers

**Note:** Customer questions and answers in red below from Keith (18 Jan 2017)

1. **Upon application of 28VDC power, how soon do each of the output signals (IRIG, 10MHz) appear?**

**Keith's response:** The SecureSync's 10 MHz output will be present moments after input power is applied. The 10 MHz output will be disciplined/aligned to GPS 1PPS within about 10 minutes or so, once the Sync LED has turned green (indicating the SecureSync is synced to GPS). Once the oscillator has locked to GPS, the Frequency Error alarm will clear, and the associated front panel red Fault LED will also extinguish (indicating all asserted alarms have now been cleared).

The IRIG output will be present within about one minute or so after applying power (once the software is up and running).

2. **Is the appearance of these signals dependent on GPS receiver lock?**

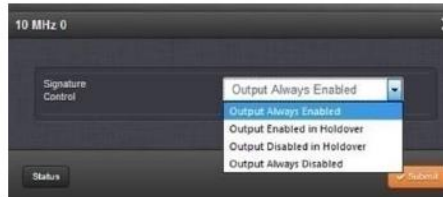
**Keith's response:** Unless “**Signature Control**” has been enabled for each of these outputs, the 10 MHz and IRIG outputs will be present, regardless of GPS receiver lock/sync state. Signature Control (which is disabled by factory default settings) is an available configuration for each individual output, which can start squelching each output (once the software is up and running) until GPS input is valid and the SecureSync has gone into sync. Signature Control is used to also squelch each output if the SecureSync loses all input references after it has achieved sync, since it was last booted-up (either right then or after a period of time of having no references available).

Note the 10 MHz output (a hardware output, not requiring the software to be running before being provided) will be present some time before the software (and therefore the Signal Control function, if enabled) can squelch this output. Once the software is up and running (and therefore Signature Control has “kicked-in”), this signal will be squelched until the SecureSync has achieved sync.

The IRIG output requires software to be up and running before it can be provided. Initially after the software is running, it will be configured using all of its default settings (IRIG B, 1kHz, Signature Control not enabled) and the output will be present. Then very shortly after the software is running, the unit will have all of its user-configurations applied (replacing the default configs as applicable). If the IRIG output's Signature Control setting has been changed from the default value (Output always enabled) to either “**Output Enabled in Holdover**” or “**Output Disabled in Holdover**” the IRIG output will be squelched at that point until sync has been achieved to an input reference.

Below for your reference are two screenshots from the web browser, just so you can see the Signature Control settings I am referring to above”

10 MHz output (Interfaces -> 10 MHz 0 page of the browser)



IRIG output (Interfaces -> IRIG output 0 page)



### Note about the available selections for Signature Control

The factory default Signature Control setting for all outputs is: **“Output Always Enabled”** (no Signature Control/squelching of this particular output occurs).

**“Output enabled in Holdover”** means this particular output is present while the SecureSync is in sync to an input reference, and also for a user-configurable allotted amount of time after losing all input references (this allotted period of time is called “Holdover”). The default allotted amount of time is 2 hours after losing all input references and then sync is completely lost if no references have been restored. This value is configured in the **Management -> Disciplining** page of the browser with a range of 1 second to 5 year). While in Holdover mode, the SecureSync remains “in sync”.

**“Output Disabled in Holdover”** means this particular output is only present while an input reference is actively present/valid. If the SecureSync goes into Holdover mode due to losing all input references, this particular output will be squelched at that point, until at least one input reference has been restored. With this setting selected, this particular output is not present while in Holdover mode.

#### 4) What is the range of time it can take for the GPS receiver to lock?

**Keith’s response:** It can take up to about 13 minutes for the SecureSync to go into GPS lock. The GPS satellites transmit a particular value (the GPS to UTC offset value) every 12.5 minutes, which needs to be received by the SecureSync’s receiver before the SecureSync can achieve sync. The length of time it takes to sync is dependent on how long before the GPS satellites transmit this value again, in relation to when the SecureSync and its receiver are powered-up.

For example, if the receiver powers up two minutes before this data is transmitted, and as long as the receiver is tracking at least four satellites (as required for a 3-D fix) it will only take 2 minutes to sync.

#### 5) What happens if we don’t issue a HALT command when powering down?

**Keith’s response:** This is a very good question, and I have some information for you that I hope will help alleviate any concerns that you may have about this:

Like any other computer, it is always best to stop the programs that are currently running before just pulling the power cord out of the computer. Otherwise, there is always that small chance that you could corrupt a program this was running at power down. So, computers usually internally stop all processes before they power-down, just to be safe. The HALT command is the method used to stop all processes in the SecureSync before powering power.

The Halt Command is provided to promote file system stability. It does take time to preserve data in the file system. Using halt to shut-down the SecureSync rather than just removing power ensures log data, and configuration information being written to the file system is successfully stored. Also, it avoids any issues of file system corruption. The file system can recover from corruption and errors. However, to avoid file system corruption the use of Halt is recommended. Also if a file error was to occur, the file system will try to fix it the next time the unit is booted up. This process could cause the power-on to take longer than normal.



---

## **\*\*Configs/configurations (Save configs /Backup and restore configs/Clean Configs)**

### **Security considerations/default and recommended configurations**

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Security- Vulnerabilities>

**Note:** The best source of info about securing/hardening the SecureSync for security is the “**Default and Recommended Configurations**” section of the online 1200 SecureSync user guide:  
[https://orolia.com/manuals/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/Conf\\_Def\\_Recom.htm](https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/ADMIN/Conf_Def_Recom.htm)

### **Factory default settings/default configs**

- Refer to “**Default and Recommended Configurations**” section of the online 1200 SecureSync user guide:  
[https://orolia.com/manuals/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/Conf\\_Def\\_Recom.htm](https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/ADMIN/Conf_Def_Recom.htm)

The factory default configurations, for “Restore Factory Defaults(Clean)” are stored in a separate directory (amongst four different directories, in this main directory).

All the factory default settings are stored in the **home/spectracom/default** directory. As shown below, the default settings are stored in the etc, home, srv and var directories as applicable (as defined by the dirlist.txt and filelist.txt files in the same default directory).

```
spadmin@CustService176 //home/spectracom/default $ ls
dirlist.txt  etc  filelist.txt  home  srv  var
```

---

### **Easily finding potential configuration issues with a customer’s unit**

Instead of side-by-side, line-by-line comparing a customer’s file to one of our files, use a third part “diff” program for Windows (such as either [WinMerge](#) or [KDiff](#)) to compare their file to a default config file. It will show all of the config changes that have been made.

---

### **\*Desire to change configs that aren’t directly accessible to the user.**

- Example: desire to alter the list of ciphers we support. Customers don’t have “access” to this via the browser.

#### **Steps**

- 1) Perform a config save.
- 2) Edit the config save.
- 3) Perform a config restore.

**Note:** the changed file(s) will be reset back to factory default if a clean is ever performed.

---

### **Configs not stored in the Compact Flash (CF) card**

**The following configuration information will remain if you remove the Compact Flash Memory card.**

- 1) The **Longitude and Latitude coordinates** will remain in the GNSS Receiver board unless you delete this information using a software command or the web UI. Position information will also be removed is a CLEAN is done on the Securesync configurations.

- 2) The **Reference Priority Table** information is held in non-volatile memory and will remain in the configuration data unless a CLEAN is done to set this back to factory defaults. This Reference Priority Table is simply a list of inputs and which have priority over each other. No specific information such as IP addresses are stored there.
- 3) All Option Cards lose their data upon power-down with the exception of one particular Option card, the 1204-12 PTP Master/Slave will retain configuration data. The card can be removed from the chassis or a FORCE/CLEAN firmware update applied to set the configuration data back to defaults. Erroneous data may also be used to overwrite your custom configurations. A handful of your Securesyncs do have this option card installed.

Here is an example of the Reference Priority Table. There is a Restore Factory Defaults button on the page that will also set any custom configurations to default. The Table is always present.

The screenshot shows the 'Configure Reference Priorities' web interface. On the left, there is an 'Actions' section with a 'Restore Factory Defaults' button. Below it is the 'Reference Status' section, which displays the status of three reference sources: GPS 0 (Priority 1), NTP 1 (Priority 2), and User 0 (Priority 3). Each source has 'TIME' and 'PPS' indicators. The main area is a table with the following data:

| Priority | Time   | 1PPS   | Enabled                             | Action |
|----------|--------|--------|-------------------------------------|--------|
| 1        | GPS 0  | GPS 0  | <input checked="" type="checkbox"/> | Delete |
| 2        | NTP 1  | NTP 1  | <input checked="" type="checkbox"/> | Delete |
| 3        | User 0 | User 0 | <input checked="" type="checkbox"/> | Delete |

At the bottom of the interface, there is a 'Reset' button on the left and a 'Submit' button on the right.

---

## \*\*Save/backup configs/restore configs/saveconf command (configuration files)

- Refer to the Config backup/restore Tech Note: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\Backup-restore configs>

**Note:** Saveconf command saves config file to: `/home/spectracom/xfer/config`

### Issues with **saveconf**

#### A) (Applicable, starting in 5.9.2?) Issue with saveconf cli command

- Refer to Salesforce Case 280992/JIRA SSS-1256 (March 2022)
- Update 5.9.4 partially broke **saveconf** command (issue with permissions)
  - **Config bundle still successfully created in the background**
  - Apparently starting in 5.9.2, **the spadmin account is no longer prompted to save the config bundle to a directory.**
  - **Temporary work-around:** perform the saveconf command. Then, after ls command shows the name of the file in the directory highlighted above, scp transfer the file out of the unit and to the desired directory in a PC (this can be temporarily added as an additional step in a script, to automate)

---

#### B) Issues associated with saveconf cli command/lockfile exists

- One “operation” which could cause the lockfile to occur, is if you are pulling the configuration bundle before a previous “Save Configuration” has finished. One of our engineers was wondering how fast are you saving/exporting the configuration bundles.
- 1. (v5.8.8 and below) Verizon Issue: lastlog is very large and archived in config bundles**
    - Fixed in 5.8.9 (per Release Notes “Fixed issue with the log file lastlog becoming too large within the configuration bundle”)
    - lockfile exists due to lastlog file getting too large with remote logins using high UIDs
    - Refer to JIRA SSS-895 (excerpt below)

This is a customer issue that Verizon was seeing - Ron Dries and I worked to track down.

##### Background

There's a file on the system, `/var/log/lastlog`, that tracks user logins. It's a sparsely populated database of users. If a user in that database has a very high UID (lets say, 2,000,000), and has attempted to log into the device, the lastlog file will report to be ~550 MB.

##### The issue

When you attempt to save a configuration bundle, if you have a lastlog file that is too large (which would happen if you have a user with a huge UID, like an LDAP user), then you will be unable to save the configuration bundle because it tries to archive `/var/log/lastlog`, which will decompress the sparsely populated database

##### The fix

Just remove the `/var/log/lastlog` entry from the filelist. This will prevent it from being added to the configuration bundle, which will prevent the disk from filling up and failing to get a bundle.

*note* there is already a "delete" line for `/var/log/*`, so if you remove `/var/log/lastlog`, then lastlog will get cleaned out whenever you run the `cfgmover.sh `clean`` operation, thus it will likely completely remove `/var/log/lastlog` from the device. There is no evidence this harms anything in our system.

#### 2. “HPNA Snapshots” (T-Mobile’s name for periodic config back-ups of their SecureSyncs)

- Per Ron Dries, “T-Mobile” periodically captures config backups of their SecureSyncs. They refer to these config backup as “**snapshots**”
- Refer to associated case **183632** for info below (this isn't the original case, but one submitted sometime after they received the patch discussed below)

- **Report for case 183632:** We fixed the Snapshot problems when launching these devices on our network w/ the software upgrade you provided (lockfile issue fixed). We are now experiencing failed snapshots again for the same reason and we need help!

### List of all files/configs that are backed-up to the saved .conf file (as spfactory account)

- In the **home/spectracom/default** directory → cat or less “filelist.txt”
- “File” items in this list are backed up to the saved.conf file. “**noarch**” and “**delete**” items are not backed-up into the saved .conf file.
- Press “q” to exit out

### Email Keith sent to Hughes after talking with Oleg (17 Nov 2014)

As far as the network configurations are concerned, these configs can be removed from one or more saved .conf files to allow cloning of SecureSyncs. This alleviates the risk of having duplicate IP address. Static values can also be changed if desired.

Otherwise, the .conf file is not intended to be edited by a user as a method to configure the SecureSyncs. One or more config files can be created from pre-configured SecureSyncs as a method to configure other SecureSyncs with similar settings. In general, the generated config file is not intended to be edited by customers. The .conf files consist of both config files as well as many rows of comma-delimited values. Incorrect editing of these non-network values can result in the need to clean the unit of call settings, resetting it back to a default state. Hardware configurations also affect the creation of the saved .conf file. If you wish to have various configurations of the SecureSync, we recommend you configure the SecureSync as desired and create a different .conf file for each desired configuration.

FYI: There is a list of all files that are placed in the .conf file. This list can be viewed via a CLI connection. To view this list cd to default directory (from home/spectracom) and then either “cat” or “less” the file of “filelist.txt”:

```

spadmin@CustService-177 /home/spectracom $ cd default
spadmin@CustService-177 /home/spectracom/default $ cat filelist.txt
#
# filelist.txt
#
# This file is used by the cfgmover.sh script to manage which configuration
# files are archived, restored, cleared, or transfered on an upgrade
#
# Operations:
# file:   Archived on an Archive operation
#        restored from selected archive on Restore operation
#        Copied from Defaults directory on Clear operation
#        (deleted if no default exists in defaults directory)

```

Each file placed in the .saved con file is annotated with “file”. Files not saved in the saved .conf are indicated with “noarch” or “delete”. As an example, below from this list are all the files associated with network settings. These files are in the .conf file.

```

Network Configuration (IPv4/IPv6)
=====
etc/dhclient-eth0.conf      file      644 root root
etc/dhclient-eth1.conf      file      644 root root
etc/dhclient-eth2.conf      file      644 root root
etc/dhclient-eth3.conf      file      644 root root
etc/route-eth0.conf         file      644 root root
etc/route-eth1.conf         file      644 root root
etc/route-eth2.conf         file      644 root root
etc/route-eth3.conf         file      644 root root
etc/conf.d/net              file      664 root root

```

---

## Limitations of config restore

- Config files created with software versions 4.8.9 or below installed cannot be restored to any software version of versions 5.0.0 or above (due to MOTD being needed. More on this further below).
- Config files created with software versions 5.0.0 or above installed cannot be restored to any previous version of software (for example, a version 5.1.5 backup file can't be applied to version 5.1.4 software).

**Note:** Trying to apply a saved config file saved from a newer version than the target unit may result in a “**Version is not found**” entry in the Update log.

---

## Potential loss of configurations: The Config file “Transfer engine” has a “20 version step” limit

- Applicable to at least software versions 5.8.2 and below. (not certain if/when a change will be incorporated, but likely it will be in 5.8.3 or 5.8.4 if a change is possible)
- Applicable to both the software update process and to config file restores.
- Loss of configurations can occur if there are more than a total of 20 software updates (both updates released to production as well as all Engineering releases not released to production- such as versions 5.4.A and 5.7A for examples) between the start version (such as v5.0.2 for instance) and the version the configs are being restored to (such as 5.8.2)

**Email Keith sent to Eric Girard (13 Nov 2018)** I wanted to make sure you are aware of something that the rest of us JUST learned, pertaining to SecureSync/9400 configs. When either performing software updates, or when installing an earlier version configuration backup bundle to a newer installed version, there is (at least currently) a “**20 version step**” limit of the configs actually being restored.

The “version steps” in between the version the configs are being restored from (such as upgrading from version 5.0.2, or restoring a config bundle which was saved at version 5.0.2 to a unit now running 5.8.2) includes all full releases, and all engineering only releases (such as version 5.4.A for instance) from that point forward to the newly installed version. If there are more than 20 total software versions between the starting version and the newer version, the config transfer engine won't restore the configs to the newer version.

But if a “step” / interim software update is first performed (which is no more than 20 versions away from the starting/current version) before updating to the latest version of software, the configs will transfer to the “step” interim version. An example of this step is to update v5.0.2 to 5.4.0 first and not just update it directly to 5.8.2.

If there are only 20 versions between the one step/interim version and the final desired version, it can then be updated from the one step to the latest version with all configs being retained. With a very early starting version (such as v5.0.2 for example) a total of like three or four software updates to interim versions is required, if its desired to retain configs being restored during an update to version 5.8.2 (as Dave Lorah just had reported to him from a customer 😊)!!!!!!

If a customer updates a SecureSync/9400 directly from v5.0.2 to 5.8.2 for instance, v5.8.2 will still be applied OK. But because there are may more than 20 versions in between, the current settings/configs will be lost when it has been upgraded to 5.8.2 (the customer will need to manually restore their desired configs)

Engineering will be looking into changing/removing this “20 step” limit on the transfer engine. But this won't be incorporated until update version 5.8.3 at the earliest. So, this 20 step limit will be in place until the change has been added into a newer version.

The biggest potential condition is if a customer is updating a remotely installed unit, from an earlier version. Then during a software update process, they then lose the settings which allow them to access it remotely.

I have asked that Dave Sohn add a notice on the same web page where customers download the software update bundles, that advises our customers that they may potentially lose configurations when applying a software update, especially when there have been no software updates applied in a very long time.

Q Does the device conduct backups of system level information, and if so, where is it stored, and can it be exported? And if changes occur, are backups taken?

A (reply from Ron Dries May 2020) Configuration backups can be initiated on the SecureSync through the CLI or webUI. The CLI will store the config bundle on the local file system where it can be copied off. The webUI will store the config bundle on the local file system as well as download it to the user's computer. This process is not scheduled by default and is a manual operation. However there are ways to automate it.

---

## Blank front panel LCD after applying a config restore

- Refer to Salesforce case 188004
- reported backup config file applied to 5.7.1 caused blank LCD/loss of all comms (including terminal connection)
- I found their bundle worked just fine here on one of our units- the real issue is the automatic reboot which occurs when restoring configs- the unit wasn't able to recover due to the compact flash card being "worn out".

---

## etc/MOTD file (Config files for software versions 5.0.0 and above)

- Starting in software version 5.0.0, the config bundles now contain an MOTD file in the /etc folder which indicates the version of software the config file was archived from.
- (search config file for "motd") Example below:

### Spectracom SecureSync Version 5.1.5

- If there is no MOTD file in the ETC folder, the backup was saved prior to version 5.0.0 and cannot be applied to units running versions 5.0.0 and above.
- If there is a MOTD file in the ETC folder, the backup was saved from a version 5.0.0 or higher unit and can be applied to units running versions 5.0.0 and above. Open the file to see the version of software it was pulled from.

**Note:** You can restore from an earlier version to a newer version (5.1.4 configs onto a 5.1.5 unit). But you can't restore from a newer version to an earlier version (5.1.5 configs onto a 5.1.4 unit). This is because any config changes that have since been incorporated aren't recognized in the earlier version. (It can actually be done, but it requires "hacking" of the backup file to make it compatible with the earlier version). I recommend updating the earlier version to 5.1.5, instead of needing to modify the backup file.

---

## Save and Restore configs using the web browser

### Limitations of config restore

- Config files created with software versions 4.8.9 or below installed cannot be restored to any software version of versions 5.0.0 or above (due to MOTD being needed. More on this further below).
- Config files created with software versions 5.0.0 or above installed cannot be restored to any previous version of software (for example, a version 5.1.5 backup file can't be applied to version 5.1.4 software).

**Note:** Trying to apply a saved config file saved from a newer version than the target unit may result in a "Version is not found" entry in the Update log.

**Note:** per Salesforce Case 193820, Perl must still be resident in the CF card for a config restore to work. If Perl was removed by previously performing the cleaner file, the config restore will not work. Refer config restore log entries further below for details on perl not being present causing restore process to fail. Performing a standard software update process (even if to the same version) will restore perl and therefore ability to perform a config restore.

### 1. Newer black/charcoal browser (v5.1.2 and above)

Left side of the Tools -> Upgrade/Backup page of the browser:



**A) To create a new config backup file:**

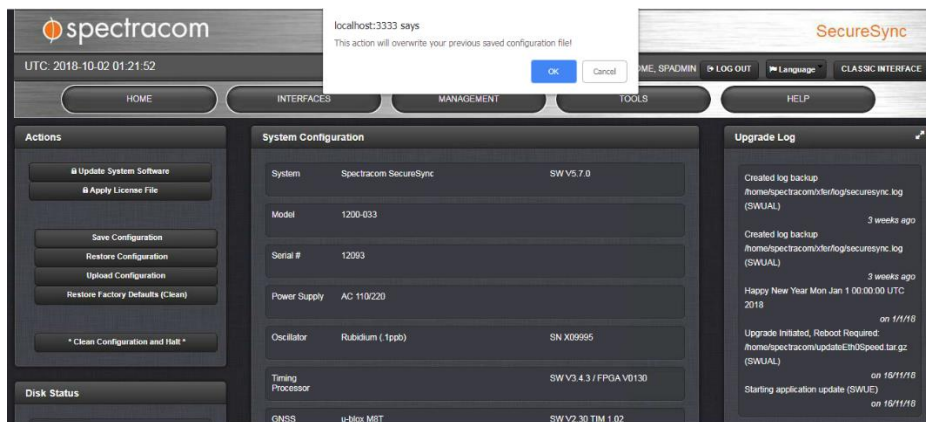
1. Press the “**Save Configuration**” button on the left side of the **Tools -> Upgrade/Backup** page

**B) To restore a previously saved config bundle:**

1. First press the **Upload Configuration** button, to load the config bundle from the PC onto the servers
2. Then press the “**Restore Configuration**” button to apply the configs, and then the unit will automatically reboot to start using the restored configs.

**“Localhost: 3333 says This action will overwrite your previous saved configuration file!”**

**Email from a customer:** While saving configuration, I'm getting following message. I'm guessing it should be fine as it will probably overwrite previously downloaded configuration, but I need your confirmation that it won't impact any current configuration/settings on the unit. As the units are deployed at client sites with live operation and I don't want to take any risk.



**Reply from Dave L (2 Oct 18)** This message is normal and informs you the Securesync will be creating a new saved Config file based on the current settings. If there was a previously saved config file it will be overwritten by this new config file.  
 This will not interrupt services and it will not change any setting on the Securesync.

## 2. Classic interface browser

- Refer to the Config backup/restore Tech Note: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\Backup-restore configs>

### A) Ability to perform remote configuration save and restore configurations via CLI interface

#### **saveconf and loadconf**

- Versions 4.8.7 and below- not available
- Version 4.8.8 (Dec 2012-ECN 3099) Added saveconf and loadconf CLI commands to handle configuration backups.

**saveconf** <file name>: Saves config file to **/home/spectracom/xfer/config**

#### Error message reported when performing saveconf command

##### (v5.8.4) “Exit: syscall failed”: Issue being observed when performing *saveconf* command

- Refer to “Error messages/conditions” further below
- Refer to JIRA ticket SSS-680

#### \*\*Manually transferring the config file (instead of using the browser to save file to Windows computer, available with the new browser starting in version 5.1.2)

- Config file must be transferred out of the SecureSync using BINARY mode. Transferring the file using ASCII mode instead will corrupt the config file, resulting in a “Version not found” error being asserted in the Update log.
- Refer to the “Update.log” section for additional info on this error message and how to verify the config file to see if it’s corrupted.

**loadconf** <file name>: Restores config file from **/home/spectracom/xfer/config** (First FTP/SCP a saved config file to this directory and then run this command).

#### Limitations of config restore

- Config files created with software versions 4.8.9 or below installed cannot be restored to any software version of versions 5.0.0 or above (due to MOTD being needed. More on this further below).
- Config files created with software versions 5.0.0 or above installed cannot be restored to any previous version of software (for example, a version 5.1.5 backup file can’t be applied to version 5.1.4 software).

**Note:** Trying to apply a saved config file saved from a newer version than the target unit may result in a “Version is not found” entry in the Update log.

#### Notes:

- **FTP** port is port 21
- **SCP** port is port 22

---

### B) Example expected log entries for a successful config restore

#### 1. Update Log



Apr 30 20:23:06 Spectracom Spectracom: [webui] Restoring config backup  
/home/spectracom/xfer/config/secsync.conf (SWUAL)  
Apr 30 21:36:51 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [webui] Restoring config backup  
/home/spectracom/xfer/config/secsync.conf (SWUAL)  
Apr 30 21:41:54 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [webui] Restoring config backup  
/home/spectracom/xfer/config/secsync.conf (SWUAL)

## 2. User Log

Apr 30 20:23:07 Spectracom shutdown[21234]: shutting down for system reboot  
Apr 30 21:41:55 P2-CP34-GPS-REV2 shutdown[12672]: shutting down for system reboot

## 3. Journal log (“[nwpdie]” entries)

Apr 30 20:24:39 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=0.  
Apr 30 20:24:40 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=1.  
Apr 30 20:24:41 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=2.  
Apr 30 20:24:41 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=3.  
Apr 30 20:24:42 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=1 Time=gps0  
1PPS=gps0.  
Apr 30 20:24:43 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=2 Time=asc0  
1PPS=asc0.  
Apr 30 20:24:43 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=3 Time=ntp  
1PPS=ntp.  
Apr 30 20:24:44 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=4 Time=user  
1PPS=user.  
Apr 30 20:25:43 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [webui] Changed Receiver Mode for GPS Reference 0 in slot  
0 from GR (0) Rcvr Mode: STANDARD (1) Dynamics: LAND (0) to GR (0) Rcvr Mode: CONTINUOUS (2) Dynamics:  
LAND (0)  
Apr 30 20:25:43 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [WEB] Changed GPSRINEX settings (spadmin)  
Apr 30 21:38:23 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=0.  
Apr 30 21:38:23 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=1.  
Apr 30 21:38:24 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=2.  
Apr 30 21:38:25 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=3.  
Apr 30 21:38:25 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=1 Time=gps0  
1PPS=gps0.  
Apr 30 21:38:26 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=2 Time=asc0  
1PPS=asc0.  
Apr 30 21:38:27 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=3 Time=ntp  
1PPS=ntp.  
Apr 30 21:38:27 P2-CP34-GPS-REV2 P2-CP34-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=4 Time=user  
1PPS=user.  
Apr 30 21:43:26 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=0.  
Apr 30 21:43:27 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=1.  
Apr 30 21:43:28 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=2.  
Apr 30 21:43:28 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Deleting entry dev=0, idx=3.  
Apr 30 21:43:29 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=1 Time=gps0  
1PPS=gps0.  
Apr 30 21:43:30 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=2 Time=asc0  
1PPS=asc0.  
Apr 30 21:43:30 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=3 Time=ntp  
1PPS=ntp.  
Apr 30 21:43:31 P2-CP35-GPS-REV2 P2-CP35-GPS-REV2.0: [nwpdie] Adding entry dev=0 enable=1 priority=4 Time=user  
1PPS=user.

## C) Error messages/conditions associated with saving config bundles

### 1) "Unable to create backup file" (SWUAL\_Lock: lockfile exists)

- Refer to SF cases such as **183632** and **175500**
- Likely due to a full CF card. Perform a **df -h** CLI command

**Email from Ron Dries (~4 Feb 2019)** pertaining to Salesforce Case 183632 (often polling config backups) Yes I do believe a reboot should clear the lockfile. This could be happening if they are pulling the configuration before a previous

configuration save has finished. One thing to check would be how fast they are saving configs. Also can you have him send the log files over

- 2) **“Exit: syscall failed “** (issue being observed in at least v5.8.5 and below when performing **saveconf** CLI command)

```
wanadmin@spectracom ~/xfer/log > ls
eclerxlog
wanadmin@spectracom ~/xfer/log $ saveconf eclerxconf
Exit: syscall failed
wanadmin@spectracom ~/xfer/log $ █
```

- Refer to Verizon case **187988** (March 2019)
- Refer to JIRA ticket **SSS-680** (created 15 Aug 2019, after 5.8.5 was released)
- The response to the saveconf command is: **“Exit: syscall failed”**
- However, this appears to be a “reporting issue” only- the config backup file is still being successfully generated, can still be exported, and can also still restore configs wsavehen applied to a unit (on 13 March, I changed System Timescale from “UTC” to “GPS” after saving configs. Applying the configs changed it back to “UTC” as expected.
- No issues observed when using the browser function to save configs
- Not confirmed, but I suspect this message MAY indicate CF card’s writes/erases have been (or are almost) used up.

**Email from Stuart Burtner (18 March 2019)** Hi Keith, The command-line command “saveconf” is OK to run in 5.8.4. The error is harmless, and telling us there’s a mistake in a configuration file for the configuration saving process (the erroneous line is ignored). Because of this mistake, it’s not saving the /etc/addlocal file inside of the configuration bundle (which shouldn’t be saved anyway). **The configuration bundle is still created.**

I’ll put a ticket in and fix it next release, but the configuration bundle will work as expected.

## D) Error messages/conditions associated with restoring config bundles

- 1) **/var/log/rc.log** (perl previously removed by the RMA process of performing the cleaner file, which removes perl, just before shipping units back to the customer)

- Refer to case 193820

**Email from Stuart B (2 May 2019)** Keith, the real problem can be seen if you check /var/log/rc.log. The “perl\_parser” startup item is trying to apply a configuration bundle to a unit.

Taken from another email I’ve sent:

In the Failed\_Device’s /var/log/rc.log:

\* Checking for Timekeeper License ...

[ ok ]

\* **Starting perl\_parser ...**

dos2unix: converting file /home/spectracom/update/transfer\_engine.pl to Unix format...

Can't locate feature.pm in @INC (you may need to install the feature module) (@INC contains: /etc/perl

/usr/local/lib/perl5/5.24.3/i686-linux /usr/local/lib/perl5/5.24.3 /usr/lib/perl5/vendor\_perl/5.24.3/i686-linux

/usr/lib/perl5/vendor\_perl/5.24.3 /usr/local/lib/perl5 /usr/lib/perl5/vendor\_perl /usr/lib/perl5/5.24.3/i686-linux

/usr/lib/perl5/5.24.3 .) at /home/spectracom/update/transfer\_engine.pl line 13.

BEGIN failed--compilation aborted at /home/spectracom/update/transfer\_engine.pl line 13.

\* **Failed to start perl\_parser**

[ !! ]

\* **ERROR: perl\_parser failed to start**

\* Setting hostname to Spectracom ...

[ ok ]

In the Working\_Device's /var/log/rc.log:

```
[ ok ]
* Wiping /tmp directory ...
[ ok ]
* Starting perl_parser ...
dos2unix: converting file /home/spectracom/update/transfer_engine.pl to Unix format...
rm: cannot remove '/transfer/conf/': Is a directory
mv: cannot stat '/transfer/conf//etc/apache2/sites_enabled/001-httpd-oldui.off': No such file or directory
groupadd: group 'spuser' already exists
groupadd: group 'spadmin' already exists
useradd: user 'spfactory' already exists
useradd: user 'spui' already exists
...
<Lots of text that isn't relevant to this case>
...
chmod: cannot access '/srv/www2/lib/Cake/Console/Templates/skel/webrootfiles': No such file or directory
chown: cannot access '/srv/www2/lib/Cake/Console/Templates/skel/webrootfiles': No such file or directory
Can't open /srv/www/xml-status/update_status.xml: No such file or directory.
[ ok ]
```

It's been determined that the update cleaner was run on these units, which strips the perl library off the device, preventing it from being able to take customer configuration bundles.

**Recovery:** Performing a standard software update process (even if to the same version) will restore perl and therefore ability to perform a config restore.

---

## 2) “ERROR: bundle version is not found”

- Refer to Salesforce Case 188403
- indicates the restore config bundle may have been captured from a unit having too early of a version when the file was generated
- Can also indicate the file that was uploaded/applied is corrupt (the unit cant extract the file)
  - Try manually extracting the config bundle- if it cant be extracted, it's a corrupt file.

**Email Keith sent to case 188403 (15 March 2019)** I'm confirming my observations with one of our Apps engineers. But it definitely appears to be a corrupt file. Once I tried applying the bundle (on two separate attempts) the Update log had an entry (“Error bundle version is not found”) indicating that the unit wasn't able to read the specific file in the bundle which reflects the software version installed in the unit that the file was generated from (at the time it was generated), so the config restore failed both times:



| ID | File            | State      | Message                                                                    |
|----|-----------------|------------|----------------------------------------------------------------------------|
| 1  | Mar 11 16:36:18 | failed     | Checking backup for updates: could not find any updates (2/2/2018)         |
| 2  | Mar 11 16:36:22 | successful | Check update status: success                                               |
| 3  | Mar 11 16:36:36 | successful | Check update status: success                                               |
| 4  | Mar 11 16:37:13 | failed     | Restoring config bundle from backup: could not find any updates (2/2/2018) |
| 5  | Mar 11 16:37:27 | successful | Check update status: success                                               |
| 6  | Mar 11 16:37:41 | successful | Check update status: success                                               |
| 7  | Mar 11 16:37:56 | failed     | Restoring config bundle from backup: could not find any updates (2/2/2018) |

As the unit first extracts the file when performing a config restore, I tried manually extracting the file you provided. I couldn't successfully extract the file manually, which explains the entries in the logs. Not sure yet on how this corrupt file could affect the SecureSync when its attempting to apply it (working with our App team on this question). But at this point, it does appear your SecureSync was highly likely adversely affected by applying a corrupt backup file.

## **\*\*Clean command (reset logs and configs)**

- Clean and Cleanhalt commands were added to the front panel “Serial” port in Archive software version 4.4.0.
- Clean and Cleanhalt commands were added to the front panel keypad in version 4.7.0

### **To perform a Clean via the front panel keypad**

#### **To clean the unit from the front panel Keypad/LCD:**

- 1) First press the front panel green check mark to see the Home menu.
- 2) Use the white directional keys to highlight the System menu and press the green check mark.
- 3) Use the white directional keys to highlight the Cmd menu and press the green check mark.
- 4) Use either the up or down keys until “clean” is displayed. Then, hit the green check key, to select it and then hit it again to apply the command. Note: An automatic reboot is performed when performing a clean command.

---

## **Desire to perform script/scripting for automating the config backup process**

- In at least 5.7.1 and below, automatically Saving/restoring configs via the SecureSync itself is not available.
- Web browser connection scripting isn't feasible to download/restore configs. But connection to the CLI (sftp/scp and telnet/ssh) can be scripted to download/upload config bundles.

**Summary:** Since the web browser interface (the normal interface used to backup or restore the configs) can't easily be scripted for automation, a user can create a custom script which logs into the CLI interface, performs a CLI command which bundles all of the configuration files into a single bundle file. Then, this bundle file can be downloaded from the time server using an FTP/SCP (file transfer) connection to the unit's CLI interface.

Custom scripts to connect to the CLI, generate the config bundle file via a CLI command, and to download the file (as well as to upload and restore a config bundle) are the responsibility of the customer.

As for the SecureSync/NetClock, these are the functions that need to be performed to download the configs using the CLI interface (and to upload/restore a config bundle), instead of using the web browser to perform these functions.

- All of the configuration files can be bundled together into a single file, which can then be exported out of the unit using an FTP/SCP client.
- A config bundle file can be uploaded into the SecureSync(s) using an FTP/SCP client. Then this config file can be restored and the unit automatically rebooted to start using its new configuration file.

**Note:** If you need a free FTP client to perform the file transfers, we often use CoreFTP lite

(<http://www.coreftp.com/>).

- The CLI command to generate the config backup file (“securesync.conf”, for both SecureSync and NetClocks) is **saveconf** <enter>.
- The ‘securesync.conf’ file is generated/stored in the following directory: /home/spectracom/xfer/config

Q (forwarded from Eric Girard) We would like to know the possibilities to automate the configuration backup of subjected devices.

**A (modified) Email Keith sent it Eric Girard (20 Jan 16)** As for the configuration backups of the SecureSyncs / NetClocks (Models 9383 and 9483), the SecureSyncs and NetClocks themselves do not have the ability to automate this desired function. The NetClock Model 9383s require the use of a GUI program to save or restore config files (our Specup utility that is also used to perform software updates). So this process can't be automated outside of the NetClock, either. This is a manual function.

However, the NetClock Model 9483s can perform a save configuration via the CLI interface (using the 'saveconf' CLI command) instead of using the web browser. And then, this saved configuration bundle file can be downloaded from the SecureSync or NetClock using FTP/SCP (Secure Copy), instead of needing to use the web browser.

You may be able to create your own custom script that can login to the CLI interface of the Model 9483 using SSH, run the **saveconf** CLI command to save the config file and then FTP into to the NetClock to download this file (the config file is created/stored in the **/home/spectracom/xfer/config** directory).

~~I have copied in Dave Sohn just so that he is aware your customer requested the capability to automate this process, and to see if he happens to have any additional info he can provide you with, that I'm not aware of.~~

Q Thanks for the procedure. So there's no way we can generate and copy out the config from our Linux server, meaning we cannot issue the "saveconf" command remote and then scp the output without any human intervention right?

A **per Dave S (2 May 17)** If you have a server that can run automated scripts, you could generate a script on that machine to periodically run the saveconf command remotely, and remotely scp that saved configuration from the unit.

## A) Below are the steps to automate/script generating and exporting the config bundle file from one or more SecureSyncs

### 1. Generate the config bundle file (using a CLI command)

1. Login to the SecureSync's CLI interface via a telnet/ssh connection (ex. PutTTY, HyperTerminal, etc.).
2. At the command prompt type **saveconf** and then press <Enter> to generate the config bundle

### 2. Download the log file from the NetClock (using an FTP/SCP client)

4. Connect to the SecureSync via a FTP/SCP client (such as CoreFTP lite for instance, a freeware program)
5. Navigate to the **/home/Spectracom/xfer/config** directory and download the **securesync.conf** file to your computer.

---

## B) Below are the steps to automate/script ploding and restoring a config bundle into one or more SecureSyncs

### 1. Upload the config bundle file into the SecureSync (using an FTP/SCP client)

1. Connect to the SecureSync via a FTP/SCP client (such as CoreFTP lite for instance, a freeware program)
2. Navigate to the **/home/Spectracom/xfer/config** directory, and upload the **securesync.conf** config bundle file from your computer into the SecureSync.

### 2. Restore the config bundle file (using a CLI command)

- Login to the SecureSync's CLI interface via a telnet/ssh connection (ex. PutTTY, HyperTerminal, etc.).
- At the command prompt, type **loadconf xyz** (where xyz is the name of the config bundle) and then press <Enter> to restore the config bundle (shortly thereafter, the unit will automatically reboot to start using the configs that were in the uploaded bundle file. It should be accessible again, within a couple minutes thereafter).

### 3. Download the log file from the NetClock (using an FTP/SCP client)

- Connect to the NetClock via a FTP/SCP client (such as CoreFTP lite for instance, a freeware program)
- Navigate to the /home/Spectracom/xfer/config directory and download the **securesync.conf** file to your computer.

**Email from Keith to Eric Girard** As for the configuration backups of the NetClocks (models 9383 and 9483), NetClocks themselves do not have the ability to automate this desired function. The NetClock Model 9383s require the use of a GUI program to save or restore config files (our Specup utility that is also used to perform updates). So, this process can't be automated outside of the NetClock, either. This is a manual function.

However, the Model 9483s can perform a save configuration via the CLI interface (using the saveconf CLI command) instead of using the web browser. And then this saved configuration file can be downloaded from the NetClock using FTP, instead of needing to use the browser.

Your customer may be able to create their own custom script that can login to the CLI interface of the Model 9483 using SSH, run the **saveconf** CLI command to save the config file and then FTP into to the NetClock to download this file (the config file is created/stored in the **/home/spectracom/xfer/config** directory).

I have copied in Dave Sohn just so that he is aware your customer requested the capability to automate this process, and to see if he happens to have any additional info he can provide you with, that I'm not aware of.

---

**Note:** As of 8/21/12, there are now Tech Notes for SecureSync and Model 9400 series backup/cloning. Refer to the applicable link below:

- Link to SecureSync config/cloning: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Backup-restore configs>
  - **Note:** The file (SecureSync.conf) is generated in: **home/spectracom/xfer/config/**
- Link to Model 9400 series config/cloning: : <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\Backup-restore configs>
- EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\Backup-restore configs
- **Note:** The file (SecureSync.conf) is generated in: **home/spectracom/xfer/config/**

The Information below is the original info, before the two Tech Notes were released:

**NOTE:** The file names are different for the SecureSync and for Model 9400 series.

- Refer to "A" below for SecureSync.
- Refer to "B" below for Model 9400 series.

**Note:** If you need a free FTP client, we often use CoreFTP Lite (<http://www.coreftp.com/>).

Note:

- **FTP port** is port 21
- **SCP port** is port 22

---

### C) SecureSync only:

**Note:** This process does not backup any installed certificates/keys.

**Important note:** The save and backup files should be transferred on and off in **BINARY** file format. With SCP, this is automatic. With FTP, must select Binary transfer mode!!

**Note:**

- FTP port is port 21
- SCP port is port 22

Tools -> “Upgrade/Backup” page of the web browser

**D) To Store/ Download configuration file for storage on a PC**

- Via CLI interface (versions 4.8.8 and above only)
  1. Type **saveconf** <enter>
  2. Then FTP/SCP the file from the directory **home/spectracom/xfer/config/SecureSync.conf**):
- Via newer web browser (v5.1.2 and above)
- Navigate to the **Tools -> Upgrade/Backup** page
- Download the config bundle by pressing “**Save Configuration**” (on the left side of the page)
- The following message will be displayed

This action will overwrite your previous saved configuration file!



- Press **OK** to download
- Save the file to the desired location on the PC.
- Via classic interface web browser: Change “Save Configuration” to “Enabled” and press Submit.

One file containing all configuration files is first generated in the SecureSync, using **Tools -> Upgrade/Backup**, page, **Configuration** tab.

The screenshot below is displayed after performing a “Store Configuration” the path to this file is displayed in this screenshot (**home/spectracom/xfer/config/SecureSync.conf**):

Creating configuration archive file /home/spectracom/xfer/config/secaresync.conf  
Validation Successful  
Please wait...

---

**E) To Restore a Configuration file:**

- Via CLI interface (versions 4.8.8 and above only)
  1. Manually FTP/SCP the saved config file to the directory **home/spectracom/xfer/config/SecureSync.conf**):
  2. Type **loadconf** <enter>
  3. The unit will automatically reboot to start using the new configs.

**1. Via the newer web browser (versions 5.1.2 and above)**

- Navigate to the **Tools** -> **Upgrade/Backup** page
- Upload config bundle into the unit by pressing: **Upload Configuration**
- Select the location of the saved config file.
- Press the **Restore Configuration** button to start using new configs.
- The unit will automatically reboot to start using new configs.

## 2. Via classic interface web browser:

4. One file containing all configuration files is first generated in the SecureSync, using **Tools** -> **Upgrade/Backup**, page, **Configuration** tab.
5. Change **“Save Configuration”** to **“Enabled”** and press Submit

When a Store configuration is performed, a file is placed in the following directory:  
[home/spectracom/xfer/config/SecureSync.conf](#).

The User can restore from this file in the directory, or they can FTP/SCP transfer the desired SecureSync.conf file from a PC into this specified SecureSync directory (such as the desire to clone or backup from an archived file).

**Note:** If performing a “Restore Configurations” before a “Store Configurations” has been performed (or a SecureSync.conf file is not present in the right directory, as described above), a validation error will occur. A “Store configuration” has to be performed first, before performing a “Restore Configuration”.

Email I sent to Richard Fox about “Restore configuration” (8/23/11). He had received a validation error because he hadn’t first performed a “Store Configuration” before performing a “Store Configuration”:

Q. I tried your first option to restore the configuration but failed at the validating process when I hit the Submit button. Do I have to be in a certain mode to do it?

Hi Richard,

The “Restore Configuration” restores configurations as they are placed in one bundled file located in the Home/Spectracom directory inside the SecureSync. Before you can perform a “Restore Configuration”, there has to be a configuration file (config) in this directory.

The first step is to perform a “Save Configuration”. This places a config file (with all configuration files bundled together in a single file) into the Home/Spectracom directory inside SecureSync. Then, if it’s desired to save this file onto a computer, you can then manually FTP (or SCP) in to this directory and copy this config file to your computer.

To “Restore Configuration” you can either restore from the file that was initially saved on that same SecureSync, or you can transfer the bundled file to the same or any other SecureSync via FTP (transfer the file using FTP to the home/spectracom directory). Then, perform a “Restore Configuration”. It will then reconfigure itself to the values that are inside the bundled file.

If you try to perform a “Restore Configuration” before performing a “Save Configuration”, there is no file to restore from, so a validation error occurs. This bundled file has to be either first created using a “Store Configuration” or the file first has to manually transferred into this directory using FTP (or SCP).

This time, it will display (I duplicated exactly what you were seeing- before performing a “Store Configuration”. I got the validation error. After performing a Store and then a Restore, I got:

Validation Successful  
 Rebooting, Please wait... Restoring from Configuration Archive File /home/spectracom/xfer/config/securesync.conf \*\*\* Rebooting ...



## F) Model 9400 series only:

**Note:** This process does not backup any installed certificates/keys.

**Important note:** The save and backup files should be transferred on and off in **BINARY** file format. With SCP, this is automatic. With FTP, must select Binary transfer mode!!

**Tools / “Upgrade/Backup”** page of the web browser

To “Store configuration” files:

One file containing all configuration files is first generated in the SecureSync, using **Tools / “Upgrade/Backup”**. Click on “Store Configuration”.

Then, if desired, this generated netclock.conf file can be manually copied out of the directory to be archived in a PC, by using FTP/SFTP /SCP.

The screenshot below is displayed after performing a “Store Configuration” the path to this file is **(/home/spectracom/xfer/config/netclock.conf)**.

### To “Restore Configuration” files:

When a Store configuration is performed, a file is placed in the following directory: **home/spectracom/xfer/config/netclock.conf**. The User can restore from this file in the directory, or they can FTP/SCP transfer the desired NetClock.conf file from a PC into this specified SecureSync directory (such as the desire to clone or backup from an archived file).

Then, perform a “Restore Configuration”.

**Note:** If performing a “Restore Configurations” before a “Store Configurations” has been performed (or a netclock.conf file is not present in the right directory, as described above), a validation error will occur. A “Store configuration” has to be performed first, before performing a “Restore Configuration”.

Email I sent to Richard Fox about “Restore configuration” (8/23/11). He had received a validation error because he hadn’t first performed a “Store Configuration” before performing a “Store Configuration”:

Q. I tried your first option to restore the configuration but failed at the validating process when I hit the Submit button. Do I have to be in a certain mode to do it?

A The “Restore Configuration” restores configurations as they are placed in one bundled file located in the Home/Spectracom directory inside the SecureSync. Before you can perform a “Restore Configuration”, there has to be a configuration file (config) in this directory.

The first step is to perform a “Save Configuration”. This places a config file (with all configuration files bundled together in a single file) into the Home/Spectracom directory inside SecureSync. Then, if it’s desired to save this file onto a computer, you can then manually FTP (or SCP) in to this directory and copy this config file to your computer.

To “Restore Configuration” you can either restore from the file that was initially saved on that same SecureSync, or you can transfer the bundled file to the same or any other SecureSync via FTP (transfer the file using FTP to the **home/spectracom** directory). Then, perform a “Restore Configuration”. It will then reconfigure itself to the values that are inside the bundled file.

If you try to perform a “Restore Configuration” before performing a “Save Configuration”, there is no file to restore from, so a validation error occurs. This bundled file has to be either first created using a “Store Configuration” or the file first has to manually transferred into this directory using FTP (or SCP).

This time, it will display (I duplicated exactly what you were seeing- before performing a “Store Configuration”. I got the validation error. After performing a Store and then a Restore, I got:

---

## After performing Save Configs, Backup Config file isn't created in the "home/spectracom/xfer/config/" directory

- CF card may be full or quite full.
- Use the **df -h** CLI command to check disk usage

### Email Keith sent to a customer (7 Aug 2014)

There is no indication displayed that the bundle file has been created. You should be able to FTP into the **home/spectracom/xfer/config/** directory, see the bundle file and transfer it out to your PC.

If by chance the file isn't in this directory, the Compact Flash card might be quite full of logs and previous update bundles. To determine what percent of the CF card is being used, connect to the CLI interface using telnet or ssh. After logging in type the following at the command prompt: **df -h** (as shown below).

```
spadmin@spectracom ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M  53% /
/dev/hda1       963M  480M  434M  53% /
devtmpfs        248M    0  248M   0% /dev
```

If the "Use%" in the "/dev/hda1" row is greater than around 70%, it may have a lot of logs and previous update bundles stored in the flash card. I haven't seen this usage ever cause a reboot to be needed, but it's good to look at this anyways before applying software updates. If it's greater than around 70% or so, let me know and I will provide you with info on how to delete past update files that remain stored in the unit after each updated.

---

## While performing Save Configs via CLI command, "tar: Removing leading '/' from member names" messages are displayed

Q. What do these messages mean?

A. The backup config process is able to truncate the full path name to the location of config files (it doesn't need to store the full path route). These entries just indicate the path was shortened. They are not an indication of a problem!

---

## While performing Save Configs with CLI command, "Cannot stat: No such file or directory" and "Exiting with failure status due to previous errors" displayed.

### Example:

```
tar: /etc/route-eth0.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
```

**Email from Oleg:** Because they do not have routes and radius activated, so the files do not exist on their system. Save configs is looking for all known possible configs and tries to copy them, some may not exist.

- The Backup process looks for specific config files to copy.
- If it can find specified files because a particular function hasn't been configured yet (such as Radius or network static routes for examples), an error message is asserted to indicate the file could not be found and then the process moves on to looking for the next file in the list.
- The "/etc/" path indication at the beginning of the "Cannot stat" message indicates which function isn't configured, resulting in the error condition being asserted

### Examples

- **/etc/route** is referring to static routes.
  - **etc/raddb/server** is referring to static routes
- These messages and error condition do not prevent the file from being built,

Q. When attempting to do it via the CLI I get the following errors...

```
admin@time ~ $ saveconf backup1
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: /etc/route-eth0.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: /etc/route-eth1.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: /etc/route-eth2.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: /etc/route-eth3.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: /etc/raddb/server: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
admin@time ~ $
```

**A. Reply from Keith after talking to Oleg (7 Aug 14)** After talking with one of our software engineers, I have some additional info for you that should help.

The Config save process looks for specific configuration files to copy into the backup bundle file. If the process doesn't find a specified file because that particular function has not yet been configured (such as Radius authentication and network routes, based on the logs you sent) it generates an error to indicate there were no files to save and moves on to the next file in the list to look for. The error should not prevent the bundle from being created.

There is no indication displayed that the bundle file has been created. You should be able to FTP into the **home/spectracom/xfer/config/** directory, see the bundle file and transfer it out to your PC.

---

## Error message when trying to "Save Configs" again (NetClock and SecureSync)

**Note:** NetClock Model 9483s versions prior to 4.8.4 can't overwrite a saved netclock.conf file (Versions 4.8.4 and above can overwrite the file). If a "save configs" has also been performed before, the saved netclock.conf file will need to be deleted first, before running the "save configs" again or else the message below is displayed (Refer to Mantis case [0001596](#) for details).

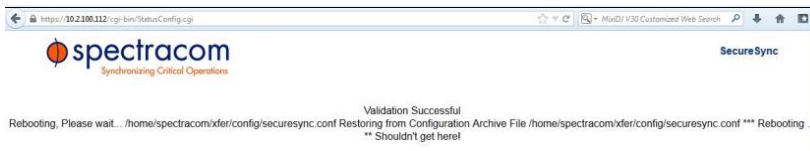
```
"Creating configuration archive file /home/spectracom/xfer/config/netclock.conf Archive file already exists, exiting... Validation Error Please check the valued and retry."
```

---

*"Shouldn't get here!" Or "An error occurred: Failed to insert session"* **error message displayed when trying to "Restore Configs" (NetClocks and SecureSync)**  
<https://na8.salesforce.com/knowledge/publishing/articleOnlineDetail.apexp?id=kA0C00000008Wlk>

- This error is due to placing a saved config file from pre-Archive version 5.0.0 onto a NetClock or SecureSync with version 5.0.0 or higher installed.

It is not recommended to apply a config backup from a version prior to version 5.0.0 and then restore it to a version of 5.0.0 or higher. If this occurs, the following partial error message will be displayed: **"shouldn't get here"** (as shown below):



### To perform a Clean via a serial connection

To reset all of the configs and logs back to factory default values, perform a “**clean**” CLI command. A “clean” command can be performed by connecting a PC running HyperTerminal (or other terminal emulator software) to the front panel SERIAL port with a straight-thru DB9F to DB9M serial cable. The settings for HyperTerminal are 9600, N, 8 1 (the “flow control” setting does not matter).

Once connected, type: **clean** <enter>. Note that this same command can also be sent with a telnet or an SSH connection (as long as these services are still enabled in the web browser). Either telnet or ssh into the NTP server and then type: **clean** <enter>. After issuing this command via RS-232, telnet or SSH, the logs and configurations will be reset and the web browser should be accessible again. Then just configure the SecureSync as desired. **Note:** An automatic reboot is performed when performing a clean command.

### FAQs about backup/restore configs (SecureSync/NetClock)

This backup process does not backup any installed certificates/keys. In version 4.8.0 and higher, the LDAP certificates are now backed-up.

- 1) It does save static assigned network settings but does not store DHCP assigned settings (it just stores the setting of DHCP being enabled).
- 2) Passwords are saved and restored/cloned.

FYI: For security and operational reasons, the save and clone configurations functions do not save or restore/clone any SSH/SSL certificates or keys. It will save and restore/clone the network settings (such as the IP address, subnet mask and gateway settings), if these are set to static values (DHCP not enabled). However, if DHCP is enabled, it will save/clone the setting of DHCP being enabled, but it won't save/clone the specific network settings. These network values will be assigned by the DHCP server when that SecureSync unit is connected to the network. Also, login passwords are stored and restored/cloned.

The reason it doesn't store/restore certificates or keys is to prevent a compromise of the private keys. The reason it doesn't store/restore DHCP assigned values is because even if the network settings were saved for either cloning of units or future restoring, it's entirely possible/likely that the DHCP server would reassign new network values anyways (especially if the values are cloned into a different unit which will have a different MAC address). So there's no benefit to saving/cloning DHCP assigned addresses.

If custom SSL certificates have been created or imported into the SecureSync, they will need to be re-created in the original or cloned SecureSync after the configuration file have been restored (or cloned into another unit). However, if no custom certificates were created or imported, the default Spectracom certificates that are present will allow operation of a cloned or configuration restored SecureSync.

(red responses below are email responses from Mike Sander, on 3/9/11 as applicable to v4.4.0 and below)

Q. Is there any way to back-up the settings using the Terminal services?

A. The first question is easy, the steps of moving the configuration archive on and off the unit are terminal based, but the creation of the configuration archive, or the action of applying an archived configuration can only be done from the web UI.

---

Q. Also I see that in section 3.7 it says this backups all but network settings. Does this include the services like DHCP and such?

A. The manual is incorrect about the second question. The network configuration is saved and restored. Users and passwords are also saved and restored. Security certificates are not saved and restored. We will be updating that configuration. (KW summary after talking to Mike S- not at this time)

The save/restore feature has two uses. The first is to make a backup of the configuration of a single unit. The second is to clone the configuring of one unit and apply it to many. The implementation is designed to meet both goals.

If the customer is using static IP addresses and they want to clone the configuration and apply it to multiple units there are several approaches they can take. The first is to clone the configuration and then change the IP addresses from the front panel to prevent multiple machines from having the same IP address. Or they could temporarily set the unit to DHCP, save that configuration, and then, after cloning that configuration onto a unit, set each one to a static IP.

**(KW summary after talking to Mike Sander):** Doesn't store DHCP settings but will store static values. The reason it doesn't store DHCP is because DHCP server could still reassign it, even if the settings were stored/restored).

### Known issues with config save

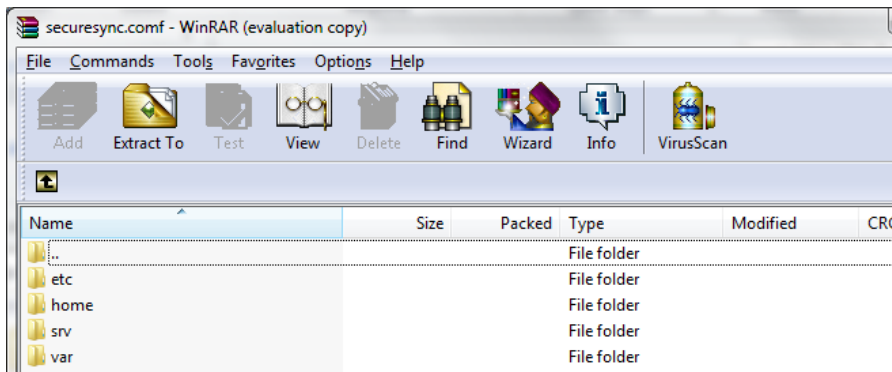
#### A) IPSec configs not being saved

- Refer to Mantis case 1853

---

### Breakdown of all the various config files

#### A) securesync.conf file



#### B) home/spectracom/config configuration files

| Config file name | Configurations for: | Notes |
|------------------|---------------------|-------|
|------------------|---------------------|-------|

|                                                      |                                                                                           |                                                                                                                                         |
|------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>access.conf</b>                                   | Network Access Restriction                                                                | <b>(Management-&gt; Network page</b> , Access Control button                                                                            |
| <b>cagps.conf</b>                                    | A-GPS (Assisted GPS)                                                                      | <b>Interfaces -&gt; GNSS 0</b> page<br>Rinex file, YUMA data                                                                            |
| <b>drdf.conf</b>                                     | Local Clock configurations                                                                | <b>Management -&gt; Time Management</b> page, Local Clocks                                                                              |
| <b>fpmcf.conf</b>                                    | Front panel LCD                                                                           | <b>Management -&gt; Front Panel</b> page<br>Content of LCD, keypad lock, menu rotation<br>enable/number of seconds to display each menu |
| <b>gpscf.conf</b>                                    | GPS Receiver                                                                              | <b>Interfaces -&gt; GNSS 0</b> page<br>Rcvr mode, constellations, offset                                                                |
| <b>gpsrinexd.conf</b>                                | A-GPS Server                                                                              | Generation of Rinex files (if AGPS Server license has been purchased/installed)                                                         |
| <b>ktsif.conf</b>                                    | MaxTFOM, Holdover, phase error limit, UTC and TAI Timescale offset                        | <b>Management -&gt; Disciplining</b> page<br><b>Management -&gt; Time Management</b> page                                               |
| <b>lccf.conf</b>                                     | Local Clock                                                                               | Local Clock settings                                                                                                                    |
| <b>lcdf.conf</b>                                     | Front panel configs                                                                       | <b>Management -&gt; Front panel</b> page                                                                                                |
| <b>nesf.conf</b>                                     | Current active alarm                                                                      | Values for active minor and major alarms                                                                                                |
| <b>notcf.conf</b>                                    | Trap and email notifications/ mask alarms                                                 | <b>Management -&gt; Notifications</b> page                                                                                              |
| <b>ofdf.conf</b> (see additional info further below) | Option Cards                                                                              | Feature mapping                                                                                                                         |
| <b>pdcf.conf</b>                                     |                                                                                           |                                                                                                                                         |
| <b>pwdcf.conf</b>                                    | Password complexity                                                                       |                                                                                                                                         |
| <b>relay.map</b>                                     | Relays                                                                                    | Model 9483 only                                                                                                                         |
| <b>remove.conf</b>                                   | Remove <b>TCPdump</b> from the system                                                     |                                                                                                                                         |
| <b>rmif.conf</b>                                     |                                                                                           |                                                                                                                                         |
| <b>rmnf.conf</b>                                     | Reference Priority table settings                                                         | <b>Management -&gt; Reference Priority</b> page                                                                                         |
| <b>rmsf.conf</b>                                     | Enable battery-backed time button                                                         | <b>Startupsync 0:</b> button is not selected<br><b>Startupsync 1:</b> button is selected                                                |
| <b>snmpd.conf</b>                                    | SNMP configs                                                                              |                                                                                                                                         |
| <b>speclog.conf</b>                                  | Log configuration/mapping (Syslog facility and Severity codes)                            |                                                                                                                                         |
| <b>rs485addr.conf</b>                                | Model 1204-0B Option Card configs                                                         |                                                                                                                                         |
| <b>stmd.conf/ stcermd.conf</b>                       | NTP Anycast mode configurations (or is it really the System Time Message daemon function) |                                                                                                                                         |
| <b>temp.conf</b>                                     | Temperature monitoring for alarms/traps                                                   | v5.3.1 and above only                                                                                                                   |
| <b>temperature.conf</b>                              | Temperature monitor for thresholds                                                        | v5.3.1 and above only (I believe)                                                                                                       |

|                   |                                                             |                                  |
|-------------------|-------------------------------------------------------------|----------------------------------|
| <b>webif.conf</b> | Browser time-out in minutes (from first accessed) I believe | Example entry "cookieTimeout 15" |
|-------------------|-------------------------------------------------------------|----------------------------------|

**ofdf.conf file**

```

cert      customize  log      update  xfer
spadmin@Spectracom ~ $ cd config
spadmin@Spectracom ~/config $ cat ofdf.conf
0,0,0,41,0,0,0
0,0,0,50,0,0,0
0,0,0,53,0,0,0
0,0,0,49,0,0,0
0,0,0,45,0,0,0
0,0,0,45,0,1,1
0,0,0,67,0,0,-1
1,31,1,47,0,0,0
1,31,1,51,0,0,0
1,31,1,51,0,1,1
1,31,1,57,0,0,0
1,31,1,57,0,1,1
2,6,2,0,0,0,0
4,1,1,58,0,0,0
4,1,1,46,0,0,0
4,1,1,53,0,0,1
5,2,1,51,0,0,2
5,2,1,44,0,0,0
6,18,1,59,0,0,0
spadmin@Spectracom ~/config $ spadmin@Spectracom

```

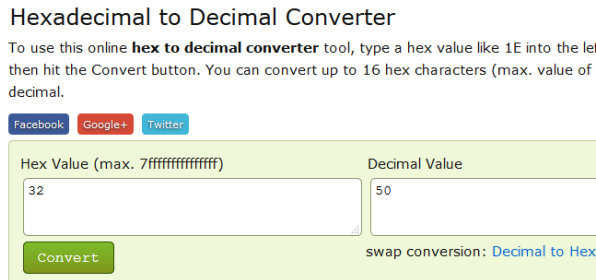
First number (1-6) in each row is the slot number. If a slot is empty, its slot number is not listed.

Second value is the Option Card Model Number (reported in decimal). Convert this decimal value to hex to determine the actual Model Number. For example, an "18" (decimal) in the list equates to "12" in hex. An "18" reported in a slot means a Model 1204-12 card is installed in that slot. (See note and dec/hex converter below the screenshot)

**Other examples**  
 "21" = 1204-15  
 "50" = 1204-32  
 "31" = 1204-1F

**Note:** Option Cards are called by their hex number, but handled in the system by the corresponding decimal value

**Example:** The 1204-32 card in the sytem is actually "50" (refer to sites such as: <http://www.binaryhexconverter.com/hex-to-decimal-converter>)



**C) home/spectracom/customize**

➤ **For Customization of the newer browser**

- For more details refer to (in this doc): [Customization of the newer browser](#)
- Newer browser can be customized with a custom logo("logo.png" file) custom language ("Locale" directory) and or custom contact info ("contact-example.html" file)
- Custom items such as a logo, locale or contact info are plced in the **home/spectracom/customize** folder (spadmin has access to this folder)

**D) /etc configuration files**

| Config file name                                               | Configurations for:                                                |
|----------------------------------------------------------------|--------------------------------------------------------------------|
| <b>conf.d folder</b>                                           | See table further below (hostname and Ethernet interface settings) |
| <b>dhclient.conf-eth number (such as "dhclient-eth0.conf")</b> | Ethernet port config files                                         |
| <b>group</b>                                                   | Account info                                                       |
| <b>host.conf</b>                                               |                                                                    |
| <b>ldap.conf</b>                                               | LDAP                                                               |
| <b>logrotate</b>                                               | Log rotation                                                       |
| <b>motd</b>                                                    | Date ("of the day")                                                |
| <b>nail.rc</b>                                                 | Nail (email settings)                                              |
| <b>nsswitch.conf</b>                                           |                                                                    |
| <b>passwd</b>                                                  |                                                                    |
| <b>policy.conf</b>                                             |                                                                    |
| <b>racoon.conf</b>                                             |                                                                    |
| <b>resolv.conf</b>                                             | Two DNS server addresses                                           |
| <b>shadow</b>                                                  | User accounts and Passwords                                        |
| <b>syslog.conf</b>                                             | Syslog configuration                                               |
| <b>tacacs_pam.conf</b>                                         | Tacacs config file                                                 |
| <b>timekeeper.conf</b>                                         | Timekeeper                                                         |
| <b>udhcpd.conf</b>                                             | Static routes??                                                    |
| <b>xinetd.conf</b>                                             | xinetd?                                                            |

#### E) /etc/apache2/

| Config file name          | Configurations for:                      | Some example parameters                                              |
|---------------------------|------------------------------------------|----------------------------------------------------------------------|
| <b>sites-enabled.conf</b> | List of supported ciphers for connection |                                                                      |
| <b>ssl.conf</b>           | SSL support for Apache                   |                                                                      |
| <b>httpd.conf</b>         | Apache config                            | PHP, languages, browser error messages, network access restrictions. |

#### F) /etc/conf.d



| Config file name | Configurations for:         |
|------------------|-----------------------------|
| hostname         | hostname                    |
| net              | Ethernet interface settings |

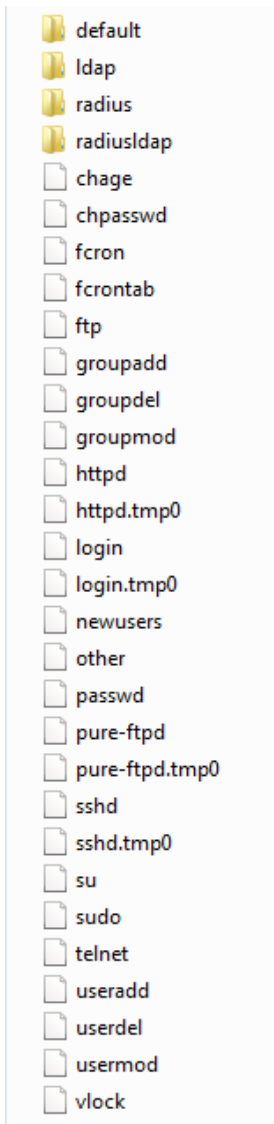
**G) /etc/local.d**

| Config file name | Configurations for: |
|------------------|---------------------|
| logrotate.conf   | Log rotations       |

**H) /etc/ntp**

| Config file name | Configurations for: |
|------------------|---------------------|
| ntp.conf         | NTP                 |
| ntp.keys         | NTP auth keys       |

**I) etc/pam.d**



### J) /etc/quagga

| Config file name  | Configurations for:              |
|-------------------|----------------------------------|
| <b>ospfd.conf</b> | OSPF for NTP over Anycast        |
| <b>bgpd.conf</b>  | BGP for NTP over Anycast         |
| <b>zebra.conf</b> | Associated with NTP over Anycast |

### K) /etc/raddb/

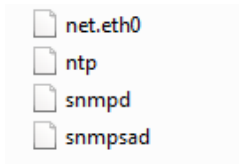
| Config file name | Configurations for:       |
|------------------|---------------------------|
| <b>server</b>    | Retries and Server adress |
| <b>rc.conf</b>   | Radius                    |

### Example Radius config file



```
server
1 #retry 3
2 165.115.19.232:1812 th1th3g 3
3
```

### L) /etc/runlevels



### M) /etc/security

| Config file name | Configurations for:    |
|------------------|------------------------|
| access.conf      | Access control for CLI |
| group.conf       |                        |
| dclimits.conf    | permissions            |
| pam_env.conf     |                        |
| time.conf        | PAM-Time module        |

### N) /etc/ssh

| Config file name   | Configurations for:           |
|--------------------|-------------------------------|
| sshd_config        | SSH                           |
| sshd_config.expert | SSH ( but not currently used) |

### O) /etc/xinetd.d/

| Config file name | Configurations for: |
|------------------|---------------------|
|                  | Daytime protocol    |
| ftp              | FTP                 |
| ssh              | ssh                 |
| telnet           | telnet              |
| time             | Time protocol       |

---

## **\*\*CLI commands to display / configure / disable the Ethernet ports (DNS, DHCP, IP address, Subnet mask, Static routes)**

### **Port state**

- Desire to display port state of all Ethernet ports (port up, port down, cable unplugged)

#### **portstate** command

**Note:** To obtain port state for SMNP instead of CLI, refer to the “**ifOperStatus**” SNMP object in the SNMP section of this document.

- CLI command is **portstate**
- Displays status of all installed Ethernet ports, including Eth0.

```
spadmin@Spectracom ~ $ portstate
eth0=Up
eth1=Unplugged
eth2=Unplugged
eth3=Unplugged
spadmin@Spectracom ~ $
```

---

### **Enable/Disable the Gigabit interfaces (eth1, eth2 or eth3)**

#### **A) Via the front panel keypad (available in versions 5.6.0 and above)**

- Refer to (in this doc): [Configure/display network settings using keypad](#)

#### **B) Via the CLI interface (required in versions 5.5.1 and below)**

#### **portset** command (available in versions 5.1.2)

- This command was implemented starting with the new web browser design in Archive version 5.1.2 (not available with earlier versions)
- The CLI command: **portset x on** enables the interface number specified by the “x”.
- The CLI command: **portset x off** disables the interface number specified by the “x”.
- CLI command to retrieve current port state: **portget x** <enter>

---

### **DNS servers (“resolv.conf” file)**

```
[admin@fsm171 etc]$ cat resolv.conf
nameserver 10.1.1.20
nameserver 10.1.1.31
[admin@fsm171 etc]$
```

### **Display/retrieve/set DNS server settings for each Ethernet interface**

- The CLI command: **dns4get x** retrieves the DNS setting (for the port specified by the “x”.
- The CLI command: **dns4set x <primary dns> <secondary dns>** configures the DNS setting for the Ethernet interface port number specified by the “x”. (note the second dns address is optional/not required)

## Display/retrieve network settings (IP address, subnet mask)

**net** <enter> shows all network settings for all ports

```
spadmin@Spectracom ~ $ net
Hostname: Spectracom
Main IPv4 default gateway (eth0): 10.2.1.1
Main IPv6 default gateway: None

eth0
MAC=00:d0:c9:ba:eb:c9
10.2.100.176/16 S
DHCPv4 (eth0)=Disabled
DG4=10.2.1.1
DNS1:10.1.1.20
INET6 fe80::2d0:c9ff:feba:ebc9/64
DHCPv6 (eth0)=Disabled

eth1 (Unplugged)
MAC=00:0c:ec:05:04:4e
10.10.202.1/16 S
DHCPv4 (eth1)=Disabled
DG4=10.10.202.254
DNS1:10.8.8.1
DHCPv6 (eth1)=Disabled

eth2
MAC=00:0c:ec:04:04:4e
10.2.100.20/16 D
DHCPv4 (eth2)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.26
DNS2:10.1.1.27
INET6 fe80::20c:ecff:fe04:44e/64
DHCPv6 (eth2)=Disabled

eth3 (Disabled)
MAC=00:0c:ec:06:04:4e
0.0.0.0/0 D
DHCPv4 (eth3)=Enabled
DG4=0.0.0.0
DHCPv6 (eth3)=Disabled
spadmin@Spectracom ~ $
```

### Subnet mask conversion table for quick-reference

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

Table 3.2: Subnet mask conversion

**net show** and **net4 / net 6** commands (net4 is equivalent to net show command in earlier Models)

**Net show** displays All IPv4 settings for all Ethernet interfaces

- **net4** displays or gets the network settings/MAC addresses for each of the network ports.
- IPv4 settings only (no IPv6 settings)

```
Spectracom NetClock 9483 Version 5.0.0
spadmin@Spectracom ~ $ net4
Hostname: Spectracom
Main IPv4 default gateway <eth0>: 10.2.100.1
eth0
00:d0:c9:c9:04:6b
10.2.100.171/16 S
DHCPv4<eth0>=Disabled
DG4=10.2.1.1
eth1
00:0c:ec:05:02:e2
10.2.100.82/16 D
DHCPv4<eth1>=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31
eth2
00:0c:ec:04:02:e2
0.0.0.0/0 S
DHCPv4<eth2>=Disabled
DG4=0.0.0.0
eth3
00:0c:ec:06:02:e2
0.0.0.0/0 D
DHCPv4<eth3>=Enabled
DG4=0.0.0.0
spadmin@Spectracom ~ $
```

Display IPv6 settings only (no IPv4 settings)

- **net6** displays the network settings/IPv6 addresses for each of the network ports.

```
eth0
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6<eth0>=Disabled
eth1
DHCPv6<eth1>=Disabled
eth2
DHCPv6<eth2>=Disabled
eth3
INET6 fe80::20c:ecff:fe06:2e2/64
DHCPv6<eth3>=Disabled
[spadmin@Spectracom ~]# net6
Spectracom
Main IPv6 default gateway: None
```

Display Eth0 settings only (Both IPv4 and IPv6 settings)

- Net settings command displays only Eth0 IPv4 and IPv6 network port configurations
- Shows no info on Eth1, Eth2, Eth3

```
[spadmin@Spectracom ~]# net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None
eth0
MAC=00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4<eth0>=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6<eth0>=Disabled
[spadmin@Spectracom ~]# net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None
```

## IPv4 Configure/show network settings

### DHCP

Get all current DHCP settings: **dhcp4get**

Get current DHCP setting for one particular port: **dhcp4get <interface>** (such as **dhcp4get 0**)

- Enable DHCP setting: **dhcp4set <interface> on** (such as **dhcp4set 0 on**)
- Disable DHCP setting: **dhcp4set <interface> off** (such as **dhcp4set 0 off**)

---

## \*\*\*\*Assigning network settings

- **IP4get <interface>** (such as **IP4get 0**)
- **IP4set <interface> <address> <mask>** (such as **IP4set 0 10.10.200.1 255.255.255.0**)
- **ip6get 1** get the IPv6 address for eth1

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

### IP Address (IPv4 and IPv6)

- **Get current IP address** (can't display all at once): **IP4get <interface>** (such as **IP4get 0**)
- Set IP address: **IP4set <interface> <address> <mask>** (such as **IP4set 0 10.10.200.1 255.255.255.0**)
- **ip6add 1** (IP xxx.xxx.xxx.xx) (subnet address xxx.xxx.xxx.xxx) (gateway address xxx.xxx.xxx.xxx)
  - a. **ip6add 1 xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx** – Adds IPv6 IP address, subnet and gateway for eth1.

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

## Gateway (Main default gateway as well as the gateway address for each port)

Get current gateway address:

- **gw4get** Displays gateway address for all Ethernet ports.
- **gw4get <interface>** (such as **gw4get 0**) for one particular gateway address
- **Note <interface>** is 0, 1, 2, 3 or m for main default gateway.

Enable and set gateway address: **gw4set <interface> <gateway address>** (example **gw4set m 10.10.200.1**)

Get (read)

- CLI command to read which port is the main default gateway: **gw4get m** <enter> (where m is for main)
- CLI command to read the gateway address for a particular Ethernet port (eth2 for example): **gw4get 2** <enter>

## Set

- CLI command to **set** which port is the main default gateway: **gw4set m x y** <enter> (where m is for “main”, x is the gateway address and y is the port number.

Example to make the default port 2: **gw4set m 10.2.1.1 2** <enter>

```

[spadmin@Spectracom ~]# net4
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1

eth0
00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4(eth0)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31

eth1
00:0c:ec:05:02:e2
0.0.0.0/0 D
DHCPv4(eth1)=Enabled
DG4=0.0.0.0
DNS1:10.1.1.20
DNS2:10.1.1.31

eth2
00:0c:ec:04:02:e2
0.0.0.0/0 D
DHCPv4(eth2)=Enabled
DG4=0.0.0.0

eth3
00:0c:ec:06:02:e2
10.10.204.1/16 S
DHCPv4(eth3)=Disabled
DG4=10.10.204.254
[spadmin@Spectracom ~]#

```

## Ifconfig / ip addr

- just type “**ifconfig**” or “**ip addr**”

**Function:** allows the operating system to setup network interfaces and allow the user to view information about the configured network interfaces.

**Displays:** all IP addresses, subnet masks, MAC addresses, received/transmitted packets, dropped packets, packet collisions, etc

### Netmask conversion table for quick-reference

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

Table 2-3: Subnet mask table



**Ifconfig -a** (Shows status of all network ports) (example below just shows a couple of the Ethernet ports)

```
Spectracom NetClock 9483 Version 4.8.8
[spadmin@Spectracom ~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:C9:C9:04:6B
          inet addr:10.2.100.3  Bcast:10.2.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2d0:c9ff:fec9:46b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4714879  errors:0  dropped:0  overruns:0  frame:0
          TX packets:2617897  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:532583302 (507.9 Mb)  TX bytes:393514456 (375.2 Mb)
          Interrupt:10  Base address:0xec00

eth1      Link encap:Ethernet  HWaddr 00:0C:EC:05:02:E2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0  errors:0  dropped:0  overruns:0  frame:0
          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11  Memory:efec0000-efee0000

eth2      Link encap:Ethernet  HWaddr 00:0C:EC:04:02:E2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0  errors:0  dropped:0  overruns:0  frame:0
          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:7  Memory:efdc0000-efde0000
```

**ifconfig eth0** (Shows only Eth0 status) – same for Eth1, Eth2 or Eth3

```
Spectracom NetClock 9483 Version 4.8.8
[spadmin@Spectracom ~]$ ipconfig eth0
-bash: ipconfig: command not found
[spadmin@Spectracom ~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:D0:C9:C9:04:6B
          inet addr:10.2.100.3  Bcast:10.2.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2d0:c9ff:fec9:46b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:887418  errors:0  dropped:0  overruns:0  frame:0
          TX packets:3841  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75307736 (71.8 Mb)  TX bytes:360429 (351.9 Kb)
          Interrupt:10  Base address:0xec00
```

**IP addr** (IP Address)

```
[spadmin@Spectracom ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: tunl0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/ipip 0.0.0.0 brd 0.0.0.0
3: sit0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
4: ip6tnl0: <NOARP> mtu 1452 qdisc noop state DOWN
    link/tunnel6 :: brd ::
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ether 00:d0:c9:c9:04:6b brd ff:ff:ff:ff:ff:ff
    inet 10.2.100.171/16 brd 10.2.255.255 scope global eth0
    inet6 fe80::2d0:c9ff:fec9:46b/64 scope link
        valid_lft forever preferred_lft forever
6: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether 00:0c:ec:05:02:e2 brd ff:ff:ff:ff:ff:ff
7: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:ec:04:02:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.251.21.135/16 brd 10.251.255.255 scope global eth2
    inet6 fe80::20c:ecff:fe04:2e2/64 scope link
        valid_lft forever preferred_lft forever
8: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether 00:0c:ec:06:02:e2 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:ecff:fe06:2e2/64 scope link
        valid_lft forever preferred_lft forever
[spadmin@Spectracom ~]$
```

## Static Routes

- Refer to "[Static Routes](#)" (Static Routing) in the "Network" section further below in this document :

---

### Holdover timeout

- Read current Holdover value: **SS\_GetHoldoverTO 0** <enter>
- Change Holdover value: **SS\_SetHoldoverTo 0 xxxx** <enter> (entered in 'seconds')

**Note:** available range is 1 second to 5 years

#### Holdover timeout is configured in "seconds"

| Desired Holdover Length | Holdover Length (in seconds) to be entered |
|-------------------------|--------------------------------------------|
| <b>2 hours</b>          | 7200 seconds (default value)               |
| <b>24 hours</b>         | 86400                                      |
| <b>7 days</b>           | 604,800                                    |
| <b>30 days</b>          | 2,419,200                                  |
| <b>1 year</b>           | 29,030,400                                 |
| <b>5 years</b>          | 10.450,944,010                             |

---

## LDAP and Radius configuration

### Radius CLI

- Not sure what software version these commands were added in.
- Type **radius** followed by the **tab** key to view the list of all radius commands

```
spadmin@Spectracom ~ $ radius
.bash_history      cert.csr           log/               server.pem.old
.bashrc            config/           mibs/             update/
.ssh/              customize/        server.crt.old    update512.tar.gz
cert/              default/          server.key.old    xfer/
```

```
Radius Configuration:           The radius configuration commands assist in
-----                        configuring radius settings
radius setretry <value>        set retry value
radius getretry                shows retry value
radius server list             list servers by <id>
radius server add <host> <port> <key> <timeout> add server
radius server del <id>        delete server
(END)
```

### LDAP CLI

- Not sure what software version these commands were added in.
- Type **ldap** followed by the **tab** key to view the list of all ldap commands

```
spadmin@Spectracom ~ $ ldap
ldapadd      ldapdelete  ldapmodify  ldappasswd  ldapurl
ldapcompare ldapexop    ldapmodrdn  ldapsearch  ldapwhoami
```

- Type a specific ldap command followed by a space and then the word **help** to see info about that command :

```
spadmin@Spectracom ~ $ ldapcompare help
usage: ldapcompare [options] DN <attr:value|attr::b64value>
where:
  DN      Distinguished Name
  attr    assertion attribute
  value   assertion value
  b64value base64 encoding of assertion value
Compare options:
```

### ldapurl:

example response: **ldap://:389** (I suspect ldap server address will be reported inside the two slashes, if it has been configured)

---

## “modinfo” Installed module/driver info(such as the e1000e network driver

- CLI command to see current version of E100e driver: **modinfo e1000e**

```

Linux 3.8.13-gentoo (Spectracom) (1)
Spectracom login: spadmin
Password:
Spectracom SecureSync Version 5.0.0
spadmin@Spectracom ~ $ modinfo
modinfo: ERROR: missing module or filename.
spadmin@Spectracom ~ $ modinfo e1000e
filename:       /lib/modules/3.8.13-gentoo/kernel/drivers/net/ethernet/intel/e1000e/e1000e.ko
version:       2.1.4-k
license:       GPL
description:   Intel(R) PRO/1000 Network Driver
author:        Intel Corporation, <linux.nics@intel.com>
srcversion:    70E6653B0A1595B95B1A08575
pci:v000008086d00001559sv*d*hc*sc*i*
alias:         pci:v000008086d0000155Asv*d*hc*sc*i*
alias:         pci:v000008086d0000153Bsv*d*hc*sc*i*
alias:         pci:v000008086d0000153Asv*d*hc*sc*i*
alias:         pci:v000008086d00001503sv*d*hc*sc*i*
alias:         pci:v000008086d00001502sv*d*hc*sc*i*

```

“free”, “free mem” (free -m) and “cat/proc/meminfo” memory commands

Scheduled leap second

- Command to get the next scheduled leap second: **CS\_GetLeapSec 0**

```

spadmin@CustService-177 ~ $ CS_GetLeapSec 0
Leap Second: +0 sec at 00:00:00 000/0000 UTC

```

**Note:** User doesn't have permission to schedule the next leap second via the cli. It needs to be scheduled via the browser

```

spadmin@CustService-177 ~ $ CS_SetLeapSec 0
-bash: /usr/bin/CS_SetLeapSec: Permission denied

```

System “Uptime”

CLI commands which report the system uptime

1. SS\_GetUptime
2. uptime

```

spadmin@Spectracom ~1$ uptime
03:57:51 up 27 days, 6:20, 1

```

3. “top” command

```

top - 15:22:16 up 17:03, 1 user, load average: 1.66, 1.48, 1.51
Tasks: 75 total, 2 running, 72 sleeping, 0 stopped, 1 zombie
Cpu(s): 49.2 us, 28.7 sy, 0.0 ni, 17.5 id, 4.3 wa, 0.0 hi, 0.3 si, 0.0 st

```

- The “top” command also reports the uptime (at the top of the response)
- Refer to [http://linux.about.com/od/commands//blcmd1\\_top.htm](http://linux.about.com/od/commands//blcmd1_top.htm)

Command to reset the Network Access table

- Version 4.4.0 (possibly before) adds a new CLI command (“**unrestrict**”) to clear the Access table. In units with 4.4.0 or higher installed, no longer need to clean all configurations. This can be performed via the CLI- it’s not available via the keypad (it’s not in the Front panel “Cmd” menu).

---

## Manually delete an update file (if can’t delete it via the browser)

- 1) Type **rm -f xxxxxx** (where xxxxxx is the file name to be deleted)

```
spadmin@Spectracom ~ $ ls -al
total 138412
drwxrwxrwx 11 root    root          4096 Sep 28 19:20 .
drwxrwxr-x  4 root    root          4096 Sep  1 22:08 ..
-rw-----  1 spadmin spadmin        108 Aug 20 14:32 .bash_history
-rw-rw-r--  1 root    root           407 Aug 20 14:44 .bashrc
drwxrwxr-x  2 root    root          4096 Sep  1 22:08 .ssh
drwxrwxr-x  3 root    root          4096 Sep  1 22:08 cert
-rw-rw-r--  1 root    root          1196 Sep  1 22:08 cert.csr
drwxrwxr-x  2 root    root          4096 Sep 27 17:54 config
drwxrwxrwx  3 root    root          4096 Sep  1 22:08 customize
drwxrwxr-x  6 root    root          4096 Sep  1 22:03 default
drwxrwxr-x  4 root    root          4096 Sep 28 18:00 log
drwxrwxr-x  2 root    root          4096 Sep  1 22:03 mibs
drwx----- 31 root    root          4096 Sep  1 22:08 update
-rw-r--r--  1 spui    root       141533106 Sep 28 19:20 update521.tar.gz
drwxrwxr-x  5 root    root          4096 Sep  1 22:03 xfer
spadmin@Spectracom ~ $ rm -f update521.tar.gz
spadmin@Spectracom ~ $ ls -al
total 56
```

---

## Ability to perform software updates via CLI interface (for scripting updates)

- Version 4.8.8 (Dec 2012-ECN 3099) Added sysupgrade CLI command to perform software updates.

Ability to perform a software upgrade via CLI command (instead of using the web browser), such as for scripting software updates

Starting in Archive software version 4.8.8, the software update can be initiated using a CLI command (issued via telnet, SSH or the front panel Serial port), instead of using the web browser, if desired. This entails performing an FTP/SCP transfer of the software update file into the SecureSync's */home/spectracom* directory **and then issuing the *sysupgrade*** CLI command to initiate the software upgrade.

The syntax for issuing the *sysupgrade* command is:

- **Standard upgrade** (Such as upgrading versions 4.8.8 to 4.8.9 for example): “sysupgrade” followed by the upgrade file name (Example: *sysupgrade update489.tar.gz*).
- **Forced upgrade** (Such as downgrading versions 4.8.9 to 4.8.8 for example, but can also be used with Standard upgrades, also): “sysupgrade force” followed by the upgrade file name (Example: *sysupgrade force update489.tar.gz*).
- **Clean upgrade** (Such as first performing a Forced upgrade from 4.8.8 to 4.8.9, for example. Then automatically resetting the NTP server back to factory default settings and deleting all log files): “sysupgrade clean” followed by the upgrade file name (Example: *sysupgrade cleanupdate489.tar.gz*).

### Note:

- **FTP port** is port 21
- **SCP port** is port 22

- 
- Base 1PPS output Enable /Disable control using “ppsctrl” command

- Version 4.8.7 (~Sept 2012) added **ppsctrl** command to enable or disable the 1PPS output on the rear panel

Q from BAE systems- Our requirement is to be able to Enable\Disable the 1PPS outputs programmatically. To do so, I use the CLI command ppsctrl. The question is, can the resultant output level of a disabled 1PPS control be programmatically set? Most times, when disabled it is 0V which is what we need. Sometimes though, it is 10V which is bad for us. It seems the level depends on where in the 1PPS pulse the output transitions to disabled.

**A Per Dave Sohn 19 Mar 15:** “We currently freeze the output at the current level, I believe, and is played out according to your report. There isn't a way to do what you want programmatically. However, depending on the responsiveness for your disable, you could perform the disable half way through the second, which would ensure that the 1PPS is already in its inactive state.

## Use of REST API to control 1PPS output(s)

**Per Dave Sohn (12 Apr 17)** These configurations can also be adjusted via the REST API that we are continuing to document. Any 1PPS or 10MHz in the system could be controlled in this way.

---

## Base 10MHz output Enable / Disable output control

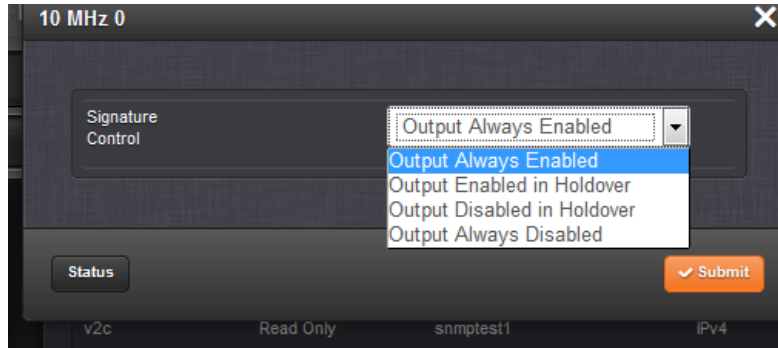
- As of at least Apr 2017 (v5.6. 0 and below), 10 MHz output is not configurable with CLI call.
- Per Dave Sohn (~9/21/12), may consider adding it with an NRE fee (or likely with very large purchase).
- Per Dave Sohn (12 Apr 17)

## Use of REST API to control 10 MHz output(s)

Per Dave Sohn (12 Apr 17) These configurations can also be adjusted via the REST API that we are continuing to document. Any 1PPS or 10MHz in the system could be controlled in this way.

## Use of web browser to control 10 MHz

➤ As of at least v5.6.0, the 10 MHz output can only be disabled via the browser (set Signature Control to "Output Always Disabled" in the **Interfaces** -> **10 MHz 0** page of the browser):



Partial email from Keith (12 Apr 17 and added to on 17 May 17) ...Currently, the 10 MHz output can only be disabled by changing the configuration of the 10 MHz Signature Control in the web browser. Signature Control for just the 10MHz output can be set to "Output Always disabled" for as long as its desired to squelch this particular output (no effects on the other outputs/functions of the system) as shown below:



However, we could consider adding a serial/CLI interface command which would also allow the output to be controlled remotely, or these settings could also be adjusted via the REST API interface.

Wade Sober can work with our SecureSync Product Manager to see what may be required (such as any associated NRE fees/minimum orders, etc) to have either a CLI command and/or REST API interface added, which can also allow the 10 MHz output to be enabled/disabled, in addition to being able to using the web browser

---

## Commands to zeroize SAASM receiver (when installed)

- Version 4.8.8 (Dec 2012-ECN 3099) Added **zeroize** command to CLI to support emergency zeroize and zeroize keys.

## CF card memory usage / “du” command

- Percent of Cf card usage can be checked using any of the following:

### 1) Web browser

**Note:** not available in classic interface

- **Tools** → **System Monitor** page of the web browser (versions **5.3.1 and above**)

Refer to the “**Percent**” field at the bottom of this section.



- **Tools** → **Upgrade/backup** page (versions 5.2.0 to 5.3.0) (under “**Disk Status**”)

### 2) CLI interface

- Type “**df**” or “**df -h**” at the command prompt (note there is a space between the “f” and the “-h”)

```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.7.1
spadmin@Spectracom ~ $ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdal       942M  419M  474M  47% /
devtmpfs        10M    0   10M   0% /dev
tmpfs           50M   448K   49M   1% /run
shm             247M    0  247M   0% /dev/shm
cgroupr_root    10M    0   10M   0% /sys/fs/cgroup
spadmin@Spectracom ~ $
```

If the “**Use%**” in the “**/dev/hda1**” row is greater than around 70%, it may have a lot of logs and previous update bundles stored in the flash card. If it’s greater than around 70% or so, let me know and I will provide you with info on how to delete past update files that remain stored in the unit after each updated.

### 3) Using SNMP

- disk usage can be also be checked via SNMP by performing an SNMP get of OID: .1.3.6.1.4.1.2021.9.1.9.1

**snmpget -v 2c -c snmpctest 10.2.100.176 .1.3.6.1.4.1.2021.9.1.9.1**

for example:



```
spadmin@Spectracom ~ $ snmpget -v 2c -c snmpptest 10.2.100.176 .1.3.6.1.4.1.2021.9.1.9.1
UCD-SNMP-MIB::dskPercent.1 = INTEGER: 47
spadmin@Spectracom ~ $
```

### Notes if the CF card is full or nearly full:

- 1) With Versions 5.2.0 (and above) **clear all logs** and **clear all stats** (bottom-left of the **Tools** -> **Upgrade/Backup** page, bottom-left corner).
  - 1) **clearlogs** and **clearstats** commands via and cli were added in version 5.1.5 (I believe). The **Clear All Logs** and **Clear all Stats** buttons were added in 5.2.1 (I believe). (bottom-left of the **Tools** -> **Upgrade/Backup** page)
  - 2) But with at least software versions 5.2.1 and below, these two buttons in the browser don't work (should be fixed in 5.30). Have to use the cli commands only to delete these items with 5.2.1 and below.
  - 3) The Temp directory may have lots of info in it. Reboot or power cycle to clear the temp directory. Run the **df -h** command again to see if the usage number has dropped because temp was cleared out.
  - 4) Run the first "du" command below to show contents of different parts of the CF card to see what Section is higher than normal. The largest directories are at the top of the list.
  - 5) Refer to the "SecureSync logs" and "SecureSync web browser" sections of this document for more information on a card.

### "du" commands (Use if the CF card is quite or completely full, such as with nullmailer tidbits)

- Refer to <http://www.cyberciti.biz/faq/how-do-i-find-the-largest-filesdirectories-on-a-linuxunixbsd-filesystem/>

**Note:** If the card is full or nearly full, to see the top 10 largest directories (and each file, in "MB) perform the first "du" command below to see the entire CF card contents. Or, go to a particular directory and perform the second "du" command to see the contents of just that directory.

### Entire contents of the CF card

At the prompt (home/spectracom directory), type the following: **du -hsx /\* | sort -rh | head -10** <enter> (where the vertical line "pipe" is SHIFT and the key under the **backspace** key)

```
Spectracom spectracom # du -hsx /* | sort -rh | head -10
```

Note it may take a few moments for the full response to be displayed.

Scroll down to the bottom (past all of the "permission denied" entries) to see the directories and their sizes. Refer to "C" below to list the content/sizes of the large directories below (such as /usr or /tmp for instance)

(Example entry below is from version 5.3.0) you can use these directory sizes to help determine which of their directories are larger than normal.

These are the directories to look at more closely (by switching to that directory and typing **ls -lh** (as discussed in more detail a little further down).

```
du: cannot access '/proc/15670': No such file or directory
du: cannot access '/proc/15672': No such file or directory
du: cannot access '/proc/15673': No such file or directory
du: cannot access '/proc/15674': No such file or directory
du: cannot access '/proc/15677': No such file or directory
319M  /usr
66M   /opt
30M   /home
22M   /srv
14M   /lib
11M   /etc
9.9M  /bin
6.0M  /sbin
4.5M  /boot
436K  /run
Spectracom spectracom # █
```

### Steps to determine CF card usage:

1. Type **du -hsx /\* | sort -rh | head -10**
2. Disregard “permission denied”
3. Scroll down to bottom of the response to see the top 10 largest directories
4. These are the directories to look at more closely (by switching to that directory and typing **ls -lh** (as discussed in more detail a little further down).
5. If **/var/nullmailer** is in the list, nullmailer is taking up too much space and needs to be cleared out.
6. See if **sqlbackup** is listed – it can be removed (**rm sqlbackup.** command
7. If **/tmp** is one of the larger directories in the list- reboot/power cycle the unit to clean this directory. The likely reason for a large **/tmp** directory is due to using tcpdump.

### Steps to clean nullmailer while logged in as spfactory

#### Gotomeeting

- A) Open Gotomeeting
- B) Sending invite to email address (add meeting in outlook)
- C) Download “desktop” (not lite, because lite can’t provide mouse and keyboard)
- D) Share keyboard and mouse
- E) Make customer the presenter
- F) Make sure to exit twice at the end to ensure out of roor user and spfactory accounts

#### THEN:

1. Login as, or switch to, spfactory user:
  - To swich from spadmin to spfactory, type: **su -l spfactory** <enter> (letter L- not i) and then enter spfactory password.
2. Switch to root user: type: **sudo su** <enter>
3. type **cd /var**<enter>
4. in /var directory, type **du -s /\* | sort -nr | head** <enter>
5. if **nullmailer** directory looks jarge, navigate to (type) **cd /var/nullmailer/queue** <enter>
6. type: **rm \*** <enter> (**while in the var/nullmailer/queue directory**)!!!!
7. Look for **sqlbackup** file in any listed directory. Delete it with **rm sqlbackup.** <enter> mmand
8. Type **df -h** <enter>

```
spectracom@spectracom ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M   53% /
/dev/hda1       963M  480M  434M   53% /
devtmpfs        248M    0  248M   0% /dev
```

9. Type **exit** <enter> to logout of root
10. Again, type **exit** <enter> to logout of spectracom

---

**Check just the contents of the current directory (such as the default directory of home/spectracom)**

**Note:** it appears this no longer works in at least 5.3.0??

- In the desired directory, type the following: **du -s \* | sort -nr** <enter> (where the vertical line “pipe” is CTRL and the key under backspace)
- Note: to see just the contents of the entire CF card (not just the current directory, see the other “du” command above).

---

**List the logs and their file sizes**

**Show the total size of the “Spectracom” logs (such as GPS Qual, Oscillator, etc)**

- 1) Type **ls -lh** at the command prompt (note there is a space between the “s” and the “-lh”)
- 2) The total size of the Spectracom logs is in the “log” row.

```
Spectracom spectracom # cd /usr
Spectracom usr # ls -lh
total 112K
drwxrwxr-x  2 root root  60K Aug 26 23:31 bin
drwxr-xr-x  2 root root  4.0K Aug 26 23:33 cli
drwxr-xr-x  5 root root  4.0K Aug 26 23:32 i686-pc-linux-gnu
drwxr-xr-x 30 root root  20K Aug 26 23:32 lib
drwxr-xr-x  6 root root  4.0K Aug 26 23:33 libexec
drwxr-xr-x  6 root root  4.0K Aug 26 23:33 local
drwxrwxr-x  2 root root  4.0K Oct 23  2014 portage
drwxr-xr-x  2 root root  4.0K Aug 26 23:32 sbin
drwxr-xr-x 51 root root  4.0K Aug 26 23:30 share
lrwxrwxrwx  1 root root    8 Aug 26 23:33 tmp -> /var/tmp
Spectracom usr #
```

**Show the total size of each of the “Spectracom” logs (such as GPS Qual, Oscillator, etc) individually**

1) Type: **ls -al /home/spectracom/log** <enter>

```
ndatopbm >
spadmin@spectracom ~$ ls -al /home/spectracom/log
total 13276
drwxrwxr-x 4 root root 4096 Sep  6 12:15 .
drwxrwxrwx 10 root root 4096 Jul 16 17:05 ..
-rw-r--r-- 1 root root 26240 Sep  6 12:05 alarms.log
-rw-r--r-- 1 root root 77763 Jul 24 05:50 alarms.log.1
-rw-r--r-- 1 root root 77280 Jul 22 13:50 alarms.log.2
-rw-r--r-- 1 root root 77280 Jul 20 14:50 alarms.log.3
-rw-r--r-- 1 root root 76955 Jul 18 13:30 alarms.log.4
-rw-r--r-- 1 root root 28769 Sep  6 14:25 auth.log
-rw-r--r-- 1 root root 22794 Sep  6 14:25 cron.log
-rw-r--r-- 1 root root 77210 Sep  6 05:30 cron.log.1
-rw-r--r-- 1 root root 77034 Sep  4 22:30 cron.log.2
-rw-r--r-- 1 root root 77219 Sep  3 15:40 cron.log.3
-rw-r--r-- 1 root root 77032 Sep  2 08:40 cron.log.4
-rw-r--r-- 1 root root 50168 Sep  6 12:05 daemon.log
-rw-r--r-- 1 root root 89082 Aug 27 15:40 daemon.log.1
-rw-r--r-- 1 root root 89670 Aug 27 14:30 daemon.log.2
-rw-r--r-- 1 root root 78498 Aug 27 13:20 daemon.log.3
-rw-r--r-- 1 root root 87906 Aug 27 12:20 daemon.log.4
drwxrwxr-x 2 root root 4096 Sep  6 14:26 discstats
-rw-r--r-- 1 root root 28530 Sep  6 12:14 events.log
-rw-r--r-- 1 root root 77204 Jul 24 08:10 events.log.1
-rw-r--r-- 1 root root 76814 Jul 23 05:50 events.log.2
-rw-r--r-- 1 root root 78628 Jul 21 20:20 events.log.3
-rw-r--r-- 1 root root 77536 Jul 20 18:40 events.log.4
-rw-r--r-- 1 root root 15280 Aug 22 12:28 journal.log
```

---

## Show all processes that are currently running (PIDs)

Type **ps -ef** at the command prompt (note there is a space between the “s” and the “-ef”)

**Note:** Can also type **ps -elf** at the command prompt for even more data

```
[spadmin@Spectracom ~]$ ps -ef
UID          PID    PPID  C  STIME TTY          TIME CMD
root           1        0  0   Sep17 ?        00:00:04 init [3]
root           2        1  0   Sep17 ?        00:00:00 [ksoftirqd/0]
root           3        1  0   Sep17 ?        00:01:34 levents/0]
root           4        1  0   Sep17 ?        00:00:00 [khelper]
root           5        1  0   Sep17 ?        00:00:00 [kthread]
root           7        5  0   Sep17 ?        00:00:00 [kblockd/0]
root          72        5  0   Sep17 ?        00:00:12 [pdflush]
root          74        5  0   Sep17 ?        00:00:00 [aio/0]
root          73        1  0   Sep17 ?        00:00:00 [kswapd0]
root         184        5  0   Sep17 ?        00:00:00 [kseriod]
root         216        5  0   Sep17 ?        00:00:00 [ata/0]
root         225        1  0   Sep17 ?        00:12:35 [kjournald]
root         463        1  0   Sep17 ?        00:00:00 udevd
root         518        1  0   Sep17 ?        00:08:41 syslogd -m 0
root         526        1  0   Sep17 ?        00:00:00 klogd
root         547        1  0   Sep17 ?        00:00:00 /usr/bin/appwatch /usr/bin/logd
root         553        547  0   Sep17 ?        00:00:12 /usr/bin/logd -n
root         819        1  0   Sep17 ?        00:00:01 /usr/sbin/xinetd
root         841        1  0   Sep17 ?        00:02:27 /usr/sbin/httd -DHTTP -DSSL -k
```

---

## “SSH”, telnet, “FTP”

- For security reasons, starting in version 5.1.3, can no longer go “outbound” with service commands (can’t telnet /ssh FROM this time server to another device. Can only telnet into this time server from another device).
- Reports “Permission denied” if attempted.

```
OpenSSH 7.6.1p1-11 Feb 2015
spadmin@Spectracom ~$ ssh
-bash: /usr/bin/ssh: Permission denied
spadmin@Spectracom ~$ ssh g
-bash: /usr/bin/ssh: Permission denied
spadmin@Spectracom ~$ ssh -G
-bash: /usr/bin/ssh: Permission denied
spadmin@Spectracom ~$ telnet
-bash: /usr/bin/telnet: Permission denied
spadmin@Spectracom ~$ telnet 10.2.100.176
-bash: /usr/bin/telnet: Permission denied
spadmin@Spectracom ~$ █
```

---

## Status of Services (such as Apache, for instance)

### rc-status command

**Note:** Run this command using SSH (not telnet). Telnet doesn’t display the left side of the response, which are the names of all the corresponding Services.

- This command checks if the previous command (i.e. the start/restart/stop of a service) executed successfully and sets the “status value”.

### Checking for just all STOPPED services

- With grep. **“-V”** causes it to search for the “opposite”
- Type **rc-status | grep started**

```

Dynamic Runlevel: manual
spadmin@Spectracom ~/log $ rc-status | grep -v started
Runlevel: default
scast485d [ stopped ]
scast485alarmd [ stopped ]
ipsetd [ stopped ]
Dynamic Runlevel: hotplugged
Dynamic Runlevel: needed
Dynamic Runlevel: manual
spadmin@Spectracom ~/log $

```

## Checking for Apache (HTTP/HTTPS)

**Note:** To check for Apache, browser must be open (login screen displayed or logged into the browser)

1. Make sure Apache2 is “started” (not “stopped”, “crashed” or “scheduled”)

```

Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ rc-status
Runlevel: default
kts [ started ]
identify [ started ]
sysklogd [ started ]
logd [ started ]
gbe-load [ started ]
net.eth0 [ started ]
net.eth1 [ inactive ]
net.eth2 [ inactive ]
net.eth3 [ inactive ]
netmount [ started ]
apache2-cert [ started ]
apache2 [ started ]
snmpd [ started ]
snmpsd [ started ]

```

2. Make sure “Apache2” is listed (**ps -el | grep apache**)

```

Spectracom spectracom # ps -el | grep apache
5 S 0 2101 1 0 80 0 - 13718 poll_s ? 00:07:32 apache2
5 S 1001 2116 2101 0 80 0 - 9415 skb_re ? 00:00:00 apache2
5 S 1001 2445 2101 0 80 0 - 15457 semtim ? 00:00:04 apache2
5 S 1001 2486 2101 0 80 0 - 14481 epoll_ ? 00:00:02 apache2
Spectracom spectracom # rc-status

```

---

## “Out-bound” network troubleshooting commands

- Refer to the following section further down for more info: Network troubleshooting from within SecureSync

Version 4.8.0 (ECN 2802) Added “out-bound” network tools to the command line interface for troubleshooting network issues associated with the SecureSync’s network.  
 Added the following network troubleshooting tool commands: ifconfig, arp, rarp, route, netstat, domainname, dig, host, nslookup and traceroute.

These commands can only be used from the front panel SERIAL port, telnet, SSH etc. They are not in the web browser.

---

## Sync/Holdover status via CLI command

**'syncstate'** command: (Added in software version 4.8.6) It prints one of three responses: **Sync**, **Holdover** or **Free Run**.

KW as of at least 2/9/12) the SecureSyncs Sync /Holdover state is not directly available via the CLI commands. It is only available via SNMP or web browser (The Status command shows Sync, but it’s the NTP sync state, not the

System's sync status).

**Update to note above:** Version 4.8.6 adds new CLI call '**syncstate**' which provides sync status.

**Email to Justin Tabeing with RT Logic (2/9/12)**

I just spoke to the engineer that implemented the front panel LCD/Keypad design and the CLI interface commands. The primary purpose of the front panel CLI interface is to provide the data to and from the front panel keypad/LCD display. The CLI was never meant to be a primary means of remotely monitoring or configuring the SecureSync. The primary method for performing these functions is via either the web browser or SNMP.

As the SecureSync's sync state is directly displayed with the state of an LED on the front panel, there was no need for a CLI command to read the sync state. So, there is no Sync/Holdover state reported via the CLI interface. However, the current Sync and Holdover states can be obtained remotely using the SNMP get functionality. If you have one or more SNMP Managers on the network, these status values can be read by the SNMP Manager, after compiling the SecureSync mib files.

Attached you should find a document that discusses the SNMP functionality of the SecureSync, in much greater detail than the user manual.

---

### Status via CLI command

'**status**' command: Shows NTP Sync status, TOM/MaxTFOM and NTP stratum level. (In software versions prior to 4.8.6, Sync state of the box is not available via CLI. Information about this is below. The fix is to upgrade to v4.8.6 or above and then use the **syncstate** CLI call (mentioned above).

(Archive Version 4.8.8 and above - see note below)

```
password
Spectracom SecureSync Version 4.8.8
[spadmin@Spectracom ~]$ status
REF:T=gps0 P=gps0
NTP:Strat=1 Sync=Y
OSC:OCKO (Trk/Lock)
TFOM=2 MaxTFOM=7
[spadmin@Spectracom ~]$
```

(Archive Version 4.8.7 and below - see note below)

```
[spadmin@Spectracom ~]$ status
REF:T=gps0 P=gps0
NTP:Strat=1 Sync=Y
OSC:OCKO (Lock)
TFOM=3 MaxTFOM=15
[spadmin@Spectracom ~]$
```

**Note:** Reported Oscillator lock State name changed (changed from "Lock" to "Trk/Lock")  
"Osc" value in this status command

(**Mantis Case 1880**) Version 4.8.8 update changed the reported state name, to also account for the newest Low Phase Noise Rb oscillator, also.

**Note in this Mantis case from Dave Sohn:** The new disciplining states associated with the low phase noise rubidium changed the lock state to track/lock to cover all oscillator cases. The procedure should be updated to reflect that.

"REF" value in the first line of the status command:

- When a value other than "Ref: None" is displayed, the SecureSync is either in full sync mode or in the Holdover mode (treated like full sync mode).
- If SecureSync is not in Sync, both of these values will change to "REF: None".
- (Versions 4.8.7 and above) If NTP is the time reference, the REF line will show BOTH the selected NTP NTP server as well as the selected PPS reference (Version 4.8.6 and below- as shown further below - only reported the selected Time Reference but not the PPS reference

```
[spadmin@fe01pdei08 cli]$ ./status
```

```
REF:T=ntp P=epp0
NTP:Strat=2 Sync=Y
OSC:Rb (Trk/Lock)
TFOM=2 MaxTFOM=15
```

(Versions 4.8.6 and below) If NTP is the selected time reference, the REF line will only show the selected NTP server (as shown in example below)

In the screenshot below, I disabled GPS (and all other input references) and made Holdover mode last only one second. This shows the result of the status message when SecureSync is out of sync (lost all references and Holdover mode expired):

```
[spadmin@Spectracom ~]# status
REF:None
NTP:Strat=1 Sync=Y
OSC:OCK0 (NoRef)
TFOM=5 MaxTFOM=15
```

**Reference Status table via CLI**

- Though limited Reference Status is available via SNMP (as of at least version 5.1.5), the status of all references can be polled via CLI interface.
- At command prompt, type: **RS\_GetStateTable 0** <enter>

```
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.5
spadmin@Spectracom - $ RS_GetStateTable 0

  Src | Time | 1PPS
-----
gps0  | 1    | 1
hst1  | 0    | 0
hst0  | 0    | 0
self  | 1    | 1
epp0  | 0    | 1
frq0  | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
      | 0    | 0
spadmin@Spectracom - $
```

- Refer to Tim Tetreault's "cheat sheet" at: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet>
- These are examples - additional calls may have since been added

| REF MONITOR commands |
|----------------------|
| RS_AddEntry          |
| RS_DeleteEntry       |
| RS_GetBestRef        |
| RS_GetEnable         |
| RS_GetEntry          |
| RS_GetPriority       |
| RS_GetStateTable     |



|                    |
|--------------------|
| RS_GetTable        |
| RS_SaveUserDef     |
| RS_SetEnable       |
| RS_SetFactDef      |
| RS_SetPriority     |
| RS_SetUserDef      |
| <b>RS_AddEntry</b> |

### NTP peers command

- At command prompt, type: **ntpq -p** <enter> (or for IP addresses only , type **ntpq -pn**)

```
Linux 3.8.13-gentoo <tul> <2>
tul login: spadmin
Password:
Spectracom NetClock 9489 Version 5.1.2
spadmin@tul ~ $ ntpq -p
      remote           refid      st t when poll reach   delay   offset  jitter
-----
+PCI_TSYNC<0>       .GPS.         0 l   1   16  377   0.000    0.014   0.002
oPPS<0>             .PPS.         1 l   -   16  377   0.000    0.000   0.002
*10.2.100.93        .GPS.         1 u   7   8   377   0.301   -0.037   0.009
+spectracom.int.    .PPS.         1 u   6   8   377   0.273    0.002   0.008
spadmin@tul ~ $
```

**Sync (“Tally Code”)**: a symbol that indicates if the listed reference is available for selection as a reference. The following table below indicates the symbols and their meanings.

#### Sync column symbols

| Symbol  | Indication                                                                                                                            |
|---------|---------------------------------------------------------------------------------------------------------------------------------------|
| *       | The Selected Time reference                                                                                                           |
| O       | The Selected PPS reference                                                                                                            |
| +       | A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected) |
| X       | “Falselticker” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).                            |
| -       | “Outlier” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).                                 |
| (blank) | Source discarded: Failed Sanity check                                                                                                 |

### GPS SAASM receiver API calls/ SAASM receiver key status (only for SAASM receivers)

#### gpsinfo:

- Reports if the SAASM receiver is zeroized or keyed.
- Reports “NOT SUPPORTED” in commercial receivers

**zeroize**: Used to zeroize the receiver of any loaded keys (same as using the front panel toggle switch)

---

## GPS reception status/troubleshooting API calls

### GPS receiver firmware version

- CLI commands: **version gps** or **gpsmdl** or **GR\_GetMfrMdl 0 0**

```
Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ version gps
Mfr/Mdl: Trimble Resolution T

GR (0) Rcv Info (66 bytes):
-----
Serial #: 2048 21427855
Date:    7/15/2011
-----
Appl Ver: 1.20
Date:    4/21/2010
-----
Core Ver: 1.26
Date:    4/21/2010
-----
spadmin@Spectracom ~ $
```

---

## GPS signal strengths (as displayed on the front panel, and with the **gpssat** command)

- CLI command: **gpssat** (in Standard/Stationary mode)
  - Will report “GNSS” with a RES-SMT receiver installed
  - Will report “GPS” with a RES-T receiver installed

```
[spadmin@Barrett_SideB ~] $ gpssat
GPS SPS 123456789ABC
Max 47 |.|.|.|.|.|.|.|.|
#Sat 9 |.|.|.|.|.|.|.|.|
Station |.|.|.|.|.|.|.|.|
```

### Standard/Stationary mode

- “Acquire” (not yet tracking any satellites while either in Mobile Mode, or Standard mode with survey complete)

```
[spadmin@Spectracom ~] $ gpssat
GPS SPS 123456789ABC
Max 50 |.|.|.|.|.|.|.|.|
#Sat 7 |.|.|.|.|.|.|.|
Acquire |.|.|.|.|.|.|.|
```

- CLI command: in Standard/Stationary mode and GPS survey is in progress
- While performing GPS survey, shows how far along the survey is (“Svy”)

```
[spadmin@Spectracom ~] $ gpssat
GPS SPS 123456789ABC
Max 48 |.|.|.|.|.|.|.|.|
#Sat 9 |.|.|.|.|.|.|.|.|
Svy 28% |.|.|.|.|.|.|.|
```

CLI command: in Standard/Stationary mode, GPS survey is complete, tracking at least one satellite

- When survey has been completed, and tracking 0 satellites (“Acquire”)
- When survey has been completed, and tracking at least one satellite (“Station”)

### Mobile mode

- **Software change to gpssat command:** Software version 5.0.0 changed **gpssat** command by removing the display of the dynamics code in Mobile mode.

### A) Software versions 5.0.0 and above, (while tracking satellites)

- In mobile mode, “Acquire” means the receiver is either not tracking any satellites or is tracking less than four satellites.
- In mobile mode, “**Mobile**” being displayed means the receiver is now tracking at least four satellites

The last line of the response indicates selected GPS mode. When in Mobile mode, because the Dynamics code for Mobile mode was removed in version 5.0.0 and above. So with versions 5.0.0 and above installed, the last line of response now just indicates “**Mobile**” when in Mobile mode and tracking at least four satellites.

```
spadmin@CustService-177 ~ $ gpssat
^[[AGPS SPS 123456789ABC
Max 49 .||.||||
#Sat 8 |||||
Mobile |||||
```

### B) Software versions 4.8.9 and below only (while tracking satellites)

- In Mobile mode, Dynamics code “**Land**”, “**Sea**” or “**Air**” being reported means the receiver’s now tracking satellites.
- Reports “**Acquire**” instead, when not tracking any satellites

The last line of the response indicates selected GPS mode (When in Mobile mode, also reports Dynamics code” “Station” is “Stationary” “Mob Lnd” is Mobile/Land

In Mobile mode or Standard mode (and while in position Hold) will display “Acquire” while tracking 0 satellites.

```
[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max 49 .||.||||
#Sat 10 |||||
Mob Lnd |||||

[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max 50 |..|||||
#Sat 10 |||||
Mob Sea |||||

[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max 50 |..|||||
#Sat 7 |||||
Mob Air |||||
```

**Email from Dave Lorah to customer (9 July 13)** The gpssat command indicates there are 9 satellites being tracked with a maximum signal strength of 47. This is a kind of a crude bar graph showing the individual signal strengths of each tracked satellite. This particular unit has good reception from one of our rooftop antennas. You should see anywhere from 5 to 9 satellites for good reception. The unit should track at least four satellites for best timing.

You can get the same information as gpssat using the front panel display. Press the green check button and then navigate to the “Display” selection. Then using the down arrow key, select “GPS INFO” and “Apply”. Use the red X key to back out to the main screen and it will show the GPS information.

### Tracking more than 12 satellites (only displays “bars” for up to 12 channels)

```
Spectracom SecureSync Version 5.8.9
spadmin@Spectracom ~ $ gpsat
GNSS 0 123456789ABC
Max 45 | .|... . .
#Sat 15 |||||...|. |
Station |||||...|
spadmin@Spectracom ~ $
```

---

GPS location (as displayed on the front panel)

CLI command: **gpsloc**

```
[spadmin@Barrett_SideB ~]$ gpsloc
Position:
Lat N 43 4 59.120
Lon W 77 35 20.522
Alt 168 m
```

---

GPS receiver Antenna Sense

**GR\_GetAntenna 0 0** <enter>

“<0> OK” indicates the GPS antenna is successfully connected to the GPS receiver ( with no opens or shorts being detected in the antenna cable).

```
31: 00 00 00 0 0 00
[spadmin@Spectracom ~]$ GR_GetAntenna 0 0
GR <0> Antenna Status: <0> OK
```

GR

Reported Number of satellites being tracked

**GR\_GetFixData 0 0** <enter>

**nSats**= Number of GPS satellites the GPS receiver is using to calculate its time and positional information

**Note:** “nSats” should normally be between 4 and 12, with typical being 6-10 satellites being tracked at all times.

```

[spadmin@Spectracom ~]$ GR_GetFixData 0 0

GR (0) Fix Data:
nSats: 9
pdop: 0.00
hdop: 0.00
vdop: 0.00
tdop: 1.00
fom: 0
tfom: 0
herr: 0
verr: 0

```

**GPS validity (indicates if the GPS receiver's reception is qualified):**

**GR\_GetValidity 0 0** <enter>

- Time and 1PPS=1 indicates GPS reception is fully qualified (desired values)
- Time and 1PPS=0 indicates GPS is not qualified (GPS survey not completed yet, or receiver is not tracking at least one satellite).

```

[spadmin@Spectracom ~]$ GR_GetValidity 0 0
Usage: GR_GetValidity <device index> <index>
[spadmin@Spectracom ~]$ GR_GetValidity 0 0

GR (0) Reference Validity:
Time: 1
1PPS: 1
[spadmin@Spectracom ~]$

```

**Satellites being tracked, signal strengths**

**GR\_GetSatData 0 0** <enter>

**ID**= Satellite identifier each channel is assigned to track (there are 12 individual channels in the GPS receiver, so only "ch" values 0 through 11 are used)

**ST**=Signal strength of that particular satellite (not 0 when satellite being tracked. Expected values 30 to 55)

**Note:** Typically, between four and 12 rows of this table should have a number other than 0 in the "st" field. In this example below, the GPS receiver is tracking 8 satellites.

GR\_  
Servser

```

[spadmin@Spectracom ~]# GR_GetSatData 0 0
GR <0> Sat Data:
  ##:  ch  id  st  t  f  fl
-----
 00:  00  29  40  0  1  00
 01:  00  30  40  0  1  00
 02:  00  14  41  0  1  00
 03:  00  25  43  0  1  00
 04:  00  16  37  0  1  00
 05:  00  32  43  0  1  00
 06:  00  20  42  0  1  00
 07:  00  31  45  0  1  00
 08:  00  00  00  0  0  00
 09:  00  00  00  0  0  00
 10:  00  00  00  0  0  00
 11:  00  00  00  0  0  00
 12:  00  00  00  0  0  00
 13:  00  00  00  0  0  00
 14:  00  00  00  0  0  00
 15:  00  00  00  0  0  00
 16:  00  00  00  0  0  00
 17:  00  00  00  0  0  00
 18:  00  00  00  0  0  00
 19:  00  00  00  0  0  00
 20:  00  00  00  0  0  00
 21:  00  00  00  0  0  00
 22:  00  00  00  0  0  00
 23:  00  00  00  0  0  00
 24:  00  00  00  0  0  00
 25:  00  00  00  0  0  00
 26:  00  00  00  0  0  00
 27:  00  00  00  0  0  00
 28:  00  00  00  0  0  00
 29:  00  00  00  0  0  00
 30:  00  00  00  0  0  00
 31:  00  00  00  0  0  00
[spadmin@Spectracom ~]#

```

**Breakdown of the Satellite Data table:**

**ch:** Receiver channel Number

**Id:** (aka “SVN” - Space Vehicle Number) ID Number of the satellite being tracked

**Distinguishing between GPS satellites and Glonass satellites, when the Glonass Option is enabled (ID field)**

To determine if each bar represents a GPS or a Glonass satellite, Mouse-hover each bar to see a report of three values (two letters, the Satellite ID number and the signal strength value for that satellite).

- **GPS satellites** are indicated with the two letters of “GP” and have a Satellite ID Number of **0 to 59**
- **Glonass satellites** are indicated with an:
  - “R” (v5.3.0 and above) or
  - the two letters of “GP” (v5.2.1 and below)
  - the two letters of “GL” and have a Satellite ID Number of 60 and above.
- **QZSS** (Japan) satellite(s) are indicated with a “J”. Note these satellites are only available in software versions v5.3.0 and above and if the Glonass option is enabled.
- **Beideu satellite(s)** are indicated with a “ ” Note these satellites are only available in software versions 5.4.0 or above, with a u-blox Model M8T receiver installed and Opt-GNS license enabled (Started shipping this ublox receiver ~17 March 2016 with approximate Serial Numbers 11718 and above).
- **Galileo** satellites (Europe) are identified with an “E”
- 

**st:** signal strength of the satellite being tracked (reported in dB/Hz, as provided by the receiver).

**t:** TRAIM (aka “bTraim”) Is this satellite accepted by the receiver’s TRAIM algorithm? (always reported as “00” with RES-T, RES-SMT and RES-SMT-GG receivers).

**f:** Fix status (aka “bInfix”) Is the receiver using this satellite in its positional fix? (“0” if not in fix, “1” if satellite is being used in fix)

**fl:** Flags reported by the receiver (always reported as “00” with RES-T, RES-SMT and RES-SMT-GG receivers).

Used only with SAASM receivers)

---

### Status of the GPS survey

**GR\_GetSurveyProg 0 0** <enter>

If the GPS receiver has been reset, a new GPS survey will start to be performed once the receiver is tracking at least four satellites. It takes about 34 minutes for survey to complete, once the GPS receiver is tracking (and continues to track) at least 4 satellites. The reported percent complete provides an estimate of how much longer before the survey completes and the SecureSync will then go back into sync (example 50% indicated about 17 minutes remain before SecureSync syncs to GPS again).

100% indicates the survey has completed successfully.

```
bash: GR_GetSurveyProg: command not found
[spadmin@Spectracom ~]$ GR_GetSurveyProg 0 0

GR (0) Survey Progress: 100%
[spadmin@Spectracom ~]$
```

---

### List of all user account (user account list): (cat /etc/passwd)

```
spadmin@SpectracomCS176 ~ $ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
news:x:9:13:news:/var/spool/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucp:/bin/false
operator:x:11:0:operator:/root:/bin/bash
portage:x:250:250:portage:/var/tmp/portage:/bin/false
nobody:x:65534:65534:nobody:/var/empty:/bin/false
sshd:x:22:22:added by portage for openssh:/var/empty:/sbin/nologin
man:x:13:15:added by portage for man-db:/usr/share/man:/sbin/nologin
cron:x:16:16:added by portage for cronbase:/var/spool/cron:/sbin/nologin
ftp:x:21:21:added by portage for ftpbase:/home/ftp:/sbin/nologin
dhcp:x:101:109:added by portage for dhcp:/var/lib/dhcp:/sbin/nologin
quagga:x:102:108:added by portage for quagga:/var/empty:/sbin/nologin
stunnel:x:103:107:added by portage for stunnel:/dev/null:/sbin/nologin
apache:x:81:81:added by portage for apache:/var/www:/sbin/nologin
ntp:x:123:123:added by portage for ntp:/dev/null:/sbin/nologin
ldap:x:439:439:added by portage for openldap:/usr/lib/openldap:/sbin/nologin
nullmailer:x:88:88:added by portage for nullmailer:/var/nullmailer:/sbin/nologin
fcron:x:104:106:added by portage for fcron:/dev/null:/sbin/nologin
mysql:x:60:60:added by portage for mysql:/dev/null:/sbin/nologin
tcpdump:x:105:105:added by portage for tcpdump:/dev/null:/sbin/nologin
messagebus:x:106:104:added by portage for dbus:/dev/null:/sbin/nologin
spfactory:x:1000:110:/:/root:/bin/bash
spui:x:1001:0:~/home/spectracom:/bin/bash
spadmin:x:1002:111:~/home/spectracom:/bin/bash
spadmin@SpectracomCS176 ~ $
```

---

### Network Services (FTP/Telnet/SSH/HTTP/HTTPS/Time/Daytime)

- View the current TCP connection timeout

```
spadmin@Spectracom ~ $ cat /proc/sys/net/ipv4/tcp_keepalive_time
7200
```

## Enable/disable Services (such as HTTPS)

- Configured in the Network/General Setup page of the browser, “Services” tab
- **servget** command displays status of all Services

```
Usage: servget <service>
service: 0=daytime protocol service
          1=time protocol service
          2=telnet service
          3=FTP service
          4=SSH service
          5=HTTP service
          6=HTTPS service
```

```
[spadmin@Spectracom ~]$ servget 6
HTTPS Service          enabled
[spadmin@Spectracom ~]$
```

- **servset** command displays status of all Services

```
Usage: servset <service> <on|off>
service: 0=daytime protocol service
          1=time protocol service
          2=telnet service
          3=FTP service
          4=SSH service
          5=HTTP service
          6=HTTPS service
```

```
[spadmin@Spectracom ~]$ servget 6
HTTPS Service          enabled
[spadmin@Spectracom ~]$ servset 6 on
[spadmin@Spectracom ~]$
```

**Note:** ECN 3173 (March 2013) adds NTP and SNMP to the list of Services that can be stopped/started or running status viewed using these two CLI commands.

```
Spectracom NetClock 9483 Version 4.8.M
[spadmin@Spectracom ~]$ servget
Invalid arguments
Usage: servget <service>
service: 0=daytime protocol service
          1=time protocol service
          2=telnet service
          3=FTP service
          4=SSH service
          5=HTTP service
          6=HTTPS service
          7=SNMP service
          8=NTP service
```

## Enable/Disable HTTPS

The CLI “Serial” port on the front of the SecureSync has an available command for verifying if HTTPS was somehow disabled and also provides the ability to re-enable any service that has been disabled. All of the available CLI commands are listed in Section 11 of the SecureSync manual (pages 11-1 through 11-3).

After connecting a straight-thru serial cable between this port and a PC running HyperTerminal, login to this port using the spadmin account and the same password used to login to the browser. Once logged in, type **services** <enter>. This command lists the services and whether or not each service is enabled. In addition to this command, **servget** <enter> can display each service one at a time and **servset** <enter> is used to re-enable or disable a particular service.



You can also use `ss` command, a well known useful utility for examining sockets in a Linux system. Run the command below to list all your open TCP and UCP ports:

```
List All Network Ports Using ss Command

$ ss -ltnu
Netid State      Recv-Q Send-Q           Local Address:Port       Peer Address:Port
udp   UNCONN      0      0             *:68                      ::*
tcp   LISTEN      0      128           :::22                     :::*
tcp   LISTEN      0      128           *:22                      ::*
tcp   LISTEN      0      50            *:3306                    ::*
tcp   LISTEN      0      128           :::80                     :::*
tcp   LISTEN      0      100          :::25                     :::*
tcp   LISTEN      0      100           *:25                      ::*
```

Make it a point to read through the man pages of the commands above for more usage information.

## Enable/disable the Classic interface browser via CLI (v5.5.0 and above)

- **servget** command displays status of all Services
- **servset 9 on** command enables the classic interface
- this variant of the `servget/servset` commands was added in version 5.5.0 update

```
admin@spectracom ~$ servget
Invalid arguments          intfc=0,1,2,3
Usage: servget <service>
  service: 0=daytime protocol service specified interface.
            1=time protocol service   intfc=0,1,2,3
            2=telnet service)         Set the IPv4 address and netmask for a
            3=FTP service              specified interface.
            4=SSH service              intfc=0,1,2,3
            5=HTTP service             addr=IPv4 address, ie 192.168.100.12
            6=HTTPS service            mask=IPv4 netmask, ie 255.255.255.0
            7=SNMP service             Display the IPv4 DNS addresses.
            8=NTP service              Set the primary and secondary IPv4 DNS
            9=Classic UI service       addresses. A missing argument will cause
                                        the corresponding DNS address to be deleted
```

## Services

### Telnet/SSH (OpenSSH)

- Refer to the online SecureSync user guide at:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/SSH\\_Configuration.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm)
- Also refer to: “\*\*SSH (for all products)” in <..\CustomerServiceAssistance.pdf>
- (Versions 5.5.1 and below require a local account be created on the box (Update version 5.6.0 added ability for Radius and tacacs to remote authenticate both the browser login and now also CLI interface, alleviating need to have an account stored on the box for CLI).

Telnet is enabled/disabled on the left side of the [Management](#) -> [Network Setup](#) page

### Emailed general info from Paul Myers (3/5/12)

#### In regards to SSH:

- We do not support any “Certificates” for SSH.
- SSH uses Public Keys.
- We allow the user to Load Public keys via the Web UI.
- The current public keys can be added to by adding text at the end of the list or by replacing entirely what is there.
- The user can create a single or list of public keys into the web browser.
- The number of public keys typically corresponds to 1 key per user. I was able to load a several key file.
- Public key length depends on the number of bits in the key and key type. A key file is typically 1-2Kbytes in my experience, but STIG compliant keys could be longer????
- Our code does not limit the length of the key file. SSH does not limit the number of public keys that I am aware of.
- A bug seems to exist in the Web UI which can cause the Web UI to fail to return after loading a LARGE key file of several kilobytes. The key file is loaded, but the connection is lost. I tried to load a 10Kbyte keyfile and the file was loaded, but I had to reconnect to the web ui. This will be investigated.

### SSH Banner (identification string, part of the SSH protocol)

- Refer to Case 250568

Q Our vendor has recently conducted a VA scan on Orolia Spectracom SecureSync OCXO 1200-213 (NTP) and found the network service banners is being displayed for port 22 SSH in which giving attackers more information to perform a targeted intrusion. We would like to know how can we disable the network service banners for port 22 SSH?

The Banner Configuration that you mentioned below is not what we’re referring to. Please see the following screenshots on the network service banners for port 22 SSH

Please see the following screenshots on the network service banners for port 22 SSH



```
C:\Users\Clarence Tong>ncat -v . . . . .
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Connected to . . . . .
SSH-2.0-OpenSSH_7.5p1-hpn14v121pk
```

**A. Reply from Dave L (5 Nov 2020)** I have some new information about this inquiry. I have been informed that SSH banner is a necessary part of the SSH protocol and is not something we have control over. The below link shows wherein the protocol it is defined. <https://unix.stackexchange.com/questions/269024/change-ssh-banner-which-is-grabbed-by-netcat> That identification string is required.

---

### limit of failed login attempts/retries for telnet/ssh

- Refer to (in this same document): [Account locked: Limit number of web browser/ssh login attempts/re-tries](#)
- 

### Network ports used for Telnet/SSH

- **Telnet:** uses TCP port 23
  - **SSH:** uses TCP port 22
- 

### SSH host keys supported

- Update version 5.4.5 (Sept 2016) added support for openSSH use of **ED25519** hostkeys
- 

### SSH (openSSH) software version installed

- Via CLI command **version ssh** <enter>
  - Via newer web browser: **Tools-> Upgrade/Backup** page (starting in update version 5.2.0)
  - Via the SecureSync software version installed
  - Refer to the “**Software Release Date**” spreadsheet at: [I:\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates](#)
- 

### libssh

- We do not install/use this package in SecureSyncs

**per Ron Dries, 24 Oct 2018** "I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync"

---

### SSH protocol versions supported (such as v1, v2, v3, etc)

- As of at least March 2018, the supported versions of SSH are not in data sheet or online user guide
- Per Dave Sohn/Ron Dries (29 Mar 2018, for at least to version 5.8.0)
  - We support **SSH v2** (SSH version 2) only
  - We **do not support SSHv1** (SSH version 1). It is considered “unsafe”
  - we do not yet support SSHv3 (SSH version 3)

Q I am currently doing network hardening of a Spectracom SecureSync 12xx NTP server to DoD standards. The listed specifications list SSH support but can you please confirm for us the SSH version? Does it support SSHv1 or SSHv2? I'm hoping it defaults to SSHv2 and that SSHv1 is not even available on your NTPs, as DoD considers SSHv1 as unsafe.

**A reply from Keith (29 Mar KW)** Thanks very much for your email and (Great) question about the Spectracom SecureSync.

I just confirmed with one of our Applications Engineers and the SecureSync Product Manager (fortunately, they were

standing next to each other) that the SecureSync ONLY supports SSH v2. It does not support SSH v1 at all (we consider it unsafe, as well!! I believe this was the answer you were hoping to hear 😊!!

*Much earlier question/answer (long before March 2018)*

Q. What is the version of the current SSH that it can support (1, 2 or both)?

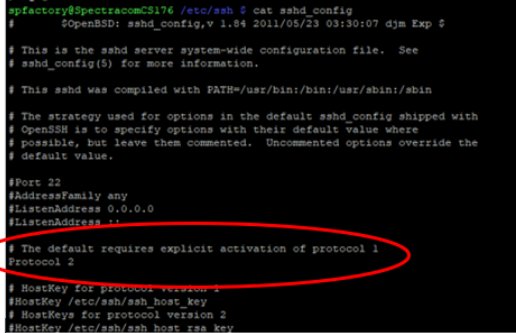
A. The SecureSync only supports SSH version 2. It does not respond to SSH version 1 (I just confirmed this by trying to connect using "V1 only").

## SSH version enabling in the sshd\_config file

(note per Keith: I believe this is correct, but confirm with Eng/Apps eng)

**cd /etc/ssh**

**cat sshd\_config**



```
apfactory@spectracom03176 /etc/ssh $ cat sshd_config
#
#OpenBSD: sshd_config,v 1.84 2011/05/23 03:30:07 djm Exp $
#
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
#
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
#
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#
# The default requires explicit activation of protocol 1
Protocol 2
#
# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
```

## Vulnerability scan findings associated with SSH

### 1. SSH Weak Message Authentication Code Algorithms?

- Refer to Salesforce Case 282790 / JIRA ticket SSS-1258 (1<sup>st</sup> reported March 2022 in v5.9.4 1200 SecureSyncs/1232 VelaSyncs)
- For more details on this weakness, refer to the same title in <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>

**Customer report (March 2022)** Our IT Security team has performed a vulnerability scan on our time servers in order to meet PCI compliance. Both our VelaSync 1232 and SecureSync 1200 devices failed with “SSH Weak Message Authentication Code Algorithms” enabled. Specifically on the following MACs: [umac-64-etm@openssh.com](mailto:umac-64-etm@openssh.com), [hmac-sha1-etm@openssh.com](mailto:hmac-sha1-etm@openssh.com), [umac-64@openssh.com](mailto:umac-64@openssh.com), hmac-sha1. The devices are running the latest available software (1.2.2 and 5.9.4 respectively). I am looking for assistance in disabling the weak codes within the SSH configuration on the devices in order to meet PCI compliance.

- A SecureSync hotpatch was created for Wegmans v5.9.4 to remove these undesired ciphers from 1200 SecureSyncs. The patch is in the JIRA ticket **SSS-1258** and also in: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software\\_patches\Disable SSH ciphers \(Wegmans JIRA SSS-1258\)](I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software_patches\Disable SSH ciphers (Wegmans JIRA SSS-1258))

## 2. Version 1.99 (sshv1) detected in v5.8.0 Nessus scan

reported by the customer, this “false alert (since v1 is not enabled) can happen in SSH versions prior to 7.6 (version 5.8.1 has SSH version 7.5p1 implemented)

I think 1.99 is an indication of backwards compatibility (i.e. support for SSH v1 & 2), so another way to ask is: Is SSH version 1 allowed? If so, can we disable it so that only SSH v2 is allowed.

Followed by...

“Looking closer, I’m thinking when you implement SSH >7.6, the SSH 1.99 issue will go away.

Here is a screen grab of our Nessus scan:

| Plugin | Plugin Name           | Family      | Severity | Protocol | Port | Exploit |
|--------|-----------------------|-------------|----------|----------|------|---------|
| SSHV1  | SSH Protocol Versions | OS::Process | Info     | TCP      | 22   | No      |

Plugin Output: The remote SSH daemon supports the following versions of the SSH protocol:

- 1.99
- 1.98
- 2.0

Description: This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### \*\*\*View the openssh config file (sshd\_config)

- Customers have permission to view this file via the spadmin account

**SSH specs/SSH configs (in the background- not available to customers)**

**SShd configuration files/SShd Expert mode**

- There are three separate sshd config files:
  - **sshd\_config**: The standard configuration file for ssh
  - **sshd\_config.all**: Spectracom-created file that Paul created back in the 9100s to allow the browser to easily update the sshd\_config with the user change to select login with keys and/or password. Note that the **sshd\_config.all** and **sshd\_config** files may not be exactly the same, but should be functionally the same
  - **sshd\_config.expert**: not currently used. Added in case we ever add an expert mode in future (we may just remove this file in the future to alleviate confusion).
- These three similar sshd config files are all located in the **/etc/ssh** directory

```
spfactory@Spectracom /etc/ssh $ ls
hostkeys.sh      ssh_config          ssh_host_rsa_key      sshd_config.expert
keysizeDSA      ssh_host_dsa_key   ssh_host_rsa_key.pub  sshd_config.key
keysizeecdsa    ssh_host_dsa_key.pub ssh_version            sshd_config.passwd
keysizeRSA      ssh_host_ecdsa_key sshd_config
moduli           ssh_host_ecdsa_key.pub sshd_config.all
spfactory@Spectracom /etc/ssh $ cat sshd_config
# $OpenBSD: sshd_config,v 1.84 2011/05/23 03:30:07 djm Exp $
```

- **SSH timeout for login (ssh idle timeout, “keepalive”, inactivity timeout)**

**NOTE:** refer also to “*Issue: SSH timeout not working*”, further below

- In at least 5.8.9 and below, SSH timeout is **hard-set in software to 7200 seconds**.

- See info further below about request/plan to add user-configurable timeout period.

➤ Refer to online SecureSync user guide:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/SSH\\_Configuration.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm)

- scroll down and select “SSH Timeout”

▼ **SSH Timeout**

The keep-SSH alive timeout is hard-set to 7200 seconds. This value is not configurable.

- Refer to **Mantis case 3019** for a request that we add an idle timeout period in a post 5.2.0 software update.

### Desire for a User-configurable SSH timeout period

- Refer to Salesforce Case 233292 and JIRA SSS-938
- Expected to be added in 5.9.1 update (as of v5.9.4, it has not been added. Jira ticket still open. I suspect it will be added to the 2400s with its wnJIRa ticket, but don't expect it to be added to the 1200s since they are going end of like.

**Status update from Tim Hammer (22 July 2020)** “Timeout is currently targeted for 5.9.1. This will be released sometime around the end of this year.”

### Issues: SSH timeout not working

I BELIEVE (but may be mistaken) SSH timeout was FIXED in 5.9.0 (with a fixed one-hour, 3600 second timeout period).

#### A) In versions such as at least 5.8.9/5.8.5/5.8.2/5.8.1/5.8.0 etc, timeout was hard-set, but was actually “indefinite” due to not working correctly

- **Refer to:** Salesforce case **175503**
- **Refer to:** JIRA ticket **SSS-548** (planned fix, as of Sept 2019 -is the v5.8.7 update)

**Case update from Stuart Burtner (25 Oct 2018)** Though the configuration file /etc/ssh/sshd\_config.all is present in 5.8.2 and in 5.7.0, I found that after two hours neither terminal disconnected.

There are likely two issues:

- 1: Saveconf doesn't save sshd\_config.all (is this an issue?)
- 2: SSH doesn't time out (ever)

My question is, what is the expected behavior? Is it one of the following:

A ssh session times out after X seconds regardless of what the customer is doing?

A ssh session times out after X seconds of inactivity (no commands issued)?

A ssh session times out after X seconds transpire and the client stopped communicating with the host?

#### B) versions around 5.2.1 and higher

- Not sure at exactly what version that this started, but this info is from v5.4.5: keepalive is hard-set to 7200 seconds (not customer-configurable)
- Refer to Mantis case 3019 for info on how to read what this value is set to.

#### C) Much earlier versions (such as 5.2.0 and below)

- With at least versions 5.0.0 and above (5.2.0 for sure), the idle timeout appears to be set to “0” which causes it to stay connected indefinitely if there is no activity.
- Refer to Mantis case 3019 for a request that we add an idle timeout period in a post 5.2.0 software update.

**“The SSH configuration is fairly standard.” Default values we change:**

- LoginGraceTime 30s: The login grace period is 30 seconds (you have 30 seconds to enter password after being prompted)
- MaxAuthTries 4: The number of password attempts is 4. (max of four failed password attempts)
- MaxStartups **3 (“3:30:10”)**: Specifies the maximum number of concurrent unauthenticated connections to the sshd daemon. Additional connections will be dropped until authentication succeeded, or the **LoginGraceTime** expires for a connection (The default is 10. We change this value to 3)

**Defaults values we don’t currently change**

➤ **Rate limiting:** SSH limits successful connection to 5 in 60 seconds.

**Note (3/9/12)** US Army has requested this value be increased in a future update. We will likely increase this value in a future release.

**Update to this (8/31/12):** The pending version 4.8.7 release addresses this.

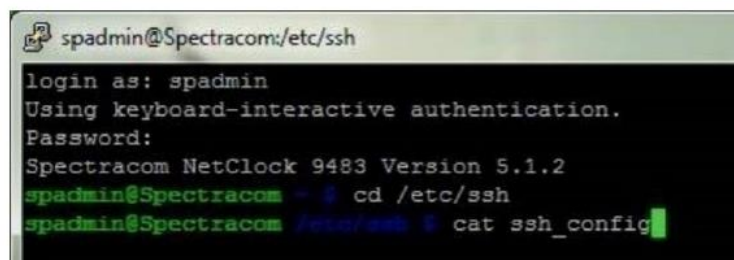
FYI- Regarding the desire to view the SecureSync's ssh\_config and sshd\_configs, these can be viewed from the SecureSync via a DB9 Serial or CLI connection.

To view these configs, either connect to the SecureSync's front panel Serial port using a DB9M to DB9F serial cable pinned straight-thru, or via a CLI connection ( via either telnet or SSH). The login credentials for the CLI interfaces is the same as the web browser. Attached is a document that discusses how to use HyperTerminal (or other terminal emulator program) to communicate with the front panel Serial port.

Then, change to the /etc/ssh file. Then you can "cat" the **sshd\_config** file. Refer to the screenshots below for an example:



```
spadmin@Spectracom:/etc/ssh
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.2
spadmin@Spectracom ~ # cd /etc/ssh
spadmin@Spectracom ~ #
```



```
spadmin@Spectracom:/etc/ssh
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.2
spadmin@Spectracom ~ # cd /etc/ssh
spadmin@Spectracom ~ # cat ssh_config
```

Hi Richard,  
Good morning. I hope you had a great weekend!

Regarding SecureSync SSH, this is not a normal means to monitor the operation of the SecureSync. SSH (Secure telnet) provides the ability to offload/upload the SecureSync's security certificates (such as the HTTPS certificate), configuration files, the unit's log files and the SNMP MIB files. It provides the same limited functionality as telnet. But with SSH, the login password is encrypted, unlike telnet which sends the password in the clear.

If you don't already have an SSH client on your PC, we typically use the PuTTY SSH client software for

Windows ( I believe this is still a freeware program). SSH uses network packets to communicate with the SecureSync.

As shown below, the following items are available via SSH:

```
10.2.100.58 - PuTTY
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom SecureSync Version 4.5.0
[spadmin@Spectracom ~]$ ls
cert.csr  config  default  log  mibs  xfer
[spadmin@Spectracom ~]$
```

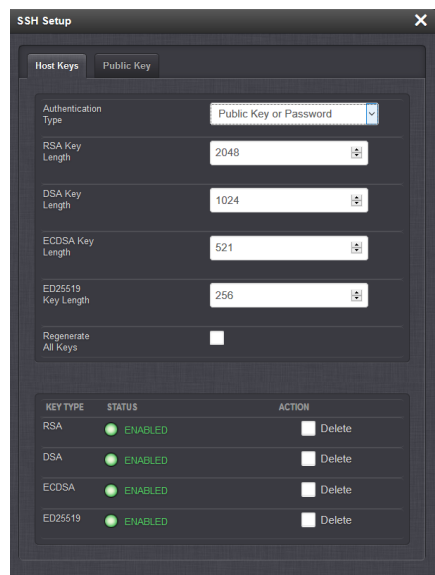
Performing an LS log (list logs) command results in:

```
10.2.100.58 - PuTTY
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom SecureSync Version 4.5.0
[spadmin@Spectracom ~]$ ls
cert.csr  config  default  log  mibs  xfer
[spadmin@Spectracom ~]$ ls log
alarms.log  cron.log.4  kern.log.1  osc.log  sys.log.2  user.log
auth.log    daemon.log  kern.log.2  qual.log  sys.log.3
cron.log    daemon.log.1  kern.log.3  snmpd.log  sys.log.4
cron.log.1  events.log  mail.log    snmpdbg.txt  system.log
cron.log.2  journal.log  ntp.log    sys.log    timing.log
cron.log.3  kern.log    ntpstats   sys.log.1  update.log
[spadmin@Spectracom ~]$
```

## SSH configurations available to users

### A) SSH configuration via the newer (black/charcoal) interface browser.

- refer to online SecureSync user guide: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/SSH\\_Configuration.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm)
- Configured in the **Management** -> **SSH Setup** page of the browser, **Host Keys** tab



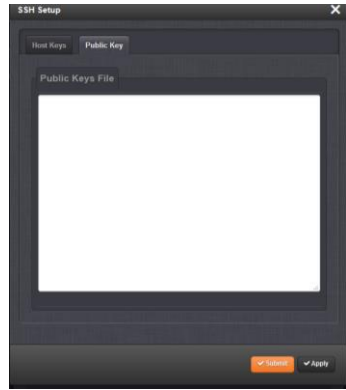
- Can login using Public Key Only, Password only, or either Public Key or Password
- When using password to connect via SSH, account and password is either the spadmin account/password or a user account that has been created.

**Note:** User accounts that are created with user rights can still connect to SSH (does not have to be assigned to the admin group)

**“Public Key Tab:** Paste the public key from each computer that wishes to access the NTP server via SSH into this field (if there are four computers, paste four keys into the table and then change “View or Edit” to Enabled. Press



Submit). Each key goes into a new line in this field).



**Note:** Private keys remain on the computers.

---

## B) SSH configuration via the classic interface browser.

- Configured in the **Network** -> **HTTPS/SSH Setup** page of the browser, **SSH** tab
- Can login using Public Key Only, Password only, or either Public Key or Password
- When using password to connect via SSH, account and password is either the spadmin account/password or a user account that has been created.

**Note:** User accounts that are created with user rights can still connect to SSH (does not have to be assigned to the admin group)

A screenshot of the 'SSH' configuration page in a browser. The page has a light gray background. At the top, there are two tabs: 'HTTPS' and 'SSH', with 'SSH' selected. Below the tabs is a section titled 'Host Keys' containing a table with the following rows:

|                            |                       |
|----------------------------|-----------------------|
| Delete Host RSA Key File   | Enabled               |
| Delete Host DSA Key File   | Disabled              |
| Delete Host ECDSA Key File | Disabled              |
| Create Host Key Files      | Disabled              |
| Host Key Status            | Valid RSA, DSA, ECDSA |
| RSA Key Length             | 2048                  |
| DSA Key Length             | 1024                  |
| ECDSA Key Length           | 521                   |

Below the table is a section titled 'SSH Authentication' with a dropdown menu for 'Authentication Type' set to 'Public Key or Password'. At the bottom is a section titled 'Public Keys File' with a dropdown menu for 'View or Edit' set to 'Disabled'.

**“Public Keys File” field:** Paste the public key from each computer that wishes to access the NTP server via SSH into this field (if there are four computers, paste four keys into the table and then change “View or Edit” to Enabled. Press Submit). Each key goes into a new line in this field).

**Note:** Private keys remain on the computers.

## SSH Expert mode

**Uses the `sshd_config.expert` configuration file**

- As of at least version 5.8.1, this mode is not available/used. It was added “just in case” we wanted to add this mode in the future.

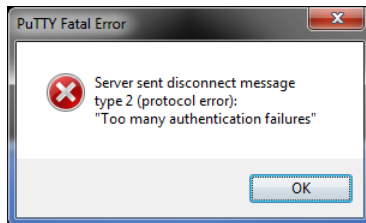
---

## Time it takes to connect (before seeing the login prompt)

| Software Version | Telnet           | SSH (with or without LDAP enabled)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.5.0            | Almost instantly | About 46 seconds or so                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 5.4.1            | Almost instantly | <p><b>Often about 2 minutes</b> (periodically, it connects in about 10-15 seconds). When logging in with a linux box, this long login results in "packet_write_wait:" and then "broken pipe" being reported:</p> <pre> Using keyboard-interactive authentication. Password: Spectracom NetClock 9483 Version 5.5.0 spfactory@Spectracom ~ \$ telnet 10.2.100.215 Trying 10.2.100.215... Connected to 10.2.100.215. Escape character is '^]'.  Linux 4.0.5-gentoo (Spectracom) (1)  Spectracom login: Password:  Login incorrect Spectracom login: Password: Connection closed by foreign host. spfactory@Spectracom ~ \$ ssh spadmin@10.2.100.215 The authenticity of host '10.2.100.215 (10.2.100.215)' can't be established. ECDSA key fingerprint is SHA256:WZLvITaZyKDFPudulnuZFyCxHwNvdA1GivRhG033a7Q. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '10.2.100.215' (ECDSA) to the list of known hosts. packet write wait: Connection to 10.2.100.215 port 22: Broken pipe spfactory@Spectracom ~ \$ ssh spadmin@10.2.100.215 Password: </pre> |

### Limit number of login Telnet/SSH re-tries (entering incorrect password several times in a row)

In summary, 3 "retries" are allowed, before a 60 second timeout period has to occur, before a successful login can occur. The following message will be displayed after the third failed login attempt ("**server sent disconnect message type 2 (protocol error): Too many authentication failures**")



**Note:** web browser login re-tries is not the same. Refer to the web browser section of this document for more info.

**Per Stuart (13 Dec 2019)** the login attempts allowed **starts at 5**, but will accumulate indefinitely until a login of said user is successful.

### Example of a similar error message response

```

$ ssh spadmin@sv02pdmi33
Password:
Received disconnect from UNKNOWN: 2: Too many authentication failures

```

**Reply from Dave Lorah (12 May 16)** I believe this is a factor of too many wrong password entries when trying to connect via SSH. I get the same error if I enter the password wrong three times in a row using Putty. Try closing the SSH viewer and reopen it.

## Telnet socket issues/Bash Shell (Reported by Walt Washington, 22 Aug 2013)

Q We are not using ssh. Our software works through this same Telnet protocol on another GPS so I know the code works. I believe the problem is the fact that your GPS runs the bash shell. We are not using a command line interface so the shell script doesn't have anywhere to run. We are simply creating a socket and connecting it through Telnet and sending ASCII characters. The connection is successful and we can see that in the GPS logs. We do not receive prompts on the Telnet connection after the connection is made like we do when we are in the command line.

Bash scripts do not return values according to my research and it is my belief that the shell is causing a disconnect since it doesn't have anywhere to run.

### Second email from Walt

The program we are using is a simple socket program written in ADA. This program was written solely for testing communication with the GPS, because once we get this working will be able to integrate it into our software product.

The socket is setup as a client and connects to the GPS server socket on port 23. There is no command line interface using this method. We have the Username and Password in separate commands. We start by connecting the socket. We then manually click the Username button to send the username. We then manually click the Password button to send the password. Then we click the Send command to attempt to get time. At any point in this process we have a receive button that we can click to see what information has been received from the GPS. When we click Connect and then receive we get some jibberish instead of a prompt for the Username. Then if we attempt to send the Username or password or the time command and then hit receive, we do not receive any information at all.

When we connect to the server, we expect to receive a prompt from the GPS for a Username. We do not receive this prompt, we only receive jibberish. We know that the program is correctly connecting to the server because the GPS logs show that the session was started and a connection was made. After that point, no matter what commands we send to the GPS, we do not get any login failures or successes. The GPS simply does not acknowledge anything we send it. Nothing changes in the logs except when we close the program it shows the session ending. We know the information is being successfully sent, because the program has error checking built in. If it tries to send the information and it does not get sent, we would get a send error.

The software version we are running is 4.8.7.

Also, using the same software, if I change the port to the FTP port (port 21) or the SSH port (port 22) we receive a welcome message from the GPS. We do not get jibberish like we do on the telnet line.

We would prefer to not use SSH or any third party software to be able to connect to the GPS.

The other GPS that we can successfully use this software with does not use the Linux Shell commands. When a telnet session is opened only simple communication back and forth occurs.

### Last email from Walt

The "gibberish" that is coming from the SecureSync is connection codes from the telnet server running on that port. It requires some response codes from their client in order to proceed further with the connection to get the username/password prompt. The links below are a discussion on a telnet vs raw socket connection, and a resource on the telnet commands/options. From a high level, the telnet server is asking the client, or socket connection in this case, to do certain things. If the client says it won't do that, it will still continue to make the connection.

<http://archive.iprodeveloper.com/forums/aft/52910>

<http://www.networksorcery.com/enp/protocol/telnet.htm>

I've attached a python script I wrote as an example showing a "WON'T" response to all of the "DO" commands, logging in, and running the HW\_GetTime command. Below is the output from the SecureSync from running the python script. The `\xff\xfd\x18` is an example of a "DO" command. The script would send back `\xff\xfc\x18` as the "WON'T" response.

Python script output:

```
"\xff\xfd\x18\xff\xfd \xff\xfd#\xff\xfd"  
\xff\xfb\x03\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x05\xff\xfd!  
\xff\xfb\x01\r\nLinux 3.8.13-gentoo (Spectracom) (1)\r\n\r\n'  
'Spectracom login: '  
'spadmin\r\nPassword: '  
'\r\nSpectracom SecureSync Version 5.0.0\r\nspadmin@Spectracom ~ $ '  
HW_GetTime 0
```

```
DOY Time:  
Year: 2013  
DOY: 235  
Hr: 18  
Min: 19
```

Sec: 47  
Nsec: 423202970  
Sync: TRUE  
spadmin@Spectracom ~ \$

---

## Troubleshooting telnet/SSH issues

General question: What software version is installed in the SecureSync/9483?

1) (First observed/reported after v5.9.0 update) SSH users don't have permissions to perform CLI commands after updating from v5.8.9

- Refer to Salesforce Cases 271486 (Aug 2021) and 261853 (Nov 2020)
- Associated with at least versions 5.9.0, 5.9.1, 5.9.2, 5.9.3 and 5.9.4.
- Refer to JIRA SSS-1142 (patch now available for v5.9.4). Refer to ("**SSH permissions in v5.9.4**")  
[\\rocfnp02\drive\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\](#)

**Status update from Tim Hammer (12 Aug 2021)**

RE: SSS-1142 (Salesforce Case 261853)

Thought I would just summarize our findings (recorded in ticket comments by Stuart) in case you want more details: We tracked the issue to an upstream change (in the sudo open source code) that we pulled in when we did the general/broad package update for 5.9.0.

The change "conflicts" with the way our cliwrapper commands works. Unfortunately, we have not identified a good way to handle the change on our side.

2) "Account locked due to **38 failed logins (count value will vary)**"

- Refer to (in this document): [Limit number of web browser/ssh login attempts/re-tries \(entering incorrect password several times in a row\)](#)

3) SSH doesn't appear to be running, even though it's enabled

- SSH daemon is not always running. It only starts running if it has detected a connection attempt is being made. Otherwise, it's not running. It can only be detected when it's actually running.

Q. sshd on one of ntp appliance is not up, reboot does not fix it.

**A (email from Keith, with input from Paul Myers, 8 Nov 2012)** In note, SSH cannot be detected unless it's actually running. And SSH is not a continuously running daemon. It doesn't continue to run, while waiting for a SSH connection to start. SSH is only started if it detects a connection attempt is in process. If you don't see SSH running, it's because SecureSync has not detected an attempt to login is now occurring. If you are trying to SSH into a SecureSync, but it's failing to connect (not even getting a login prompt), there may be a firewall blocking the SSH port, for instance. You may need to perform a wireshark packet sniff to see where the SSH packets are being lost.

**Email from Keith (9 Feb 16)** When you try connecting via ssh, does it display any error messages (such as "connection **refused**" for example)? Do you get to the login prompt but it's not taking your credentials to get past login? Or does it stop after logging in?

There are no known issues associated with SSH in version 5.2.1. With the unit still being accessible via its browser, as long as SSH is still enabled and as long as no entries have been added to the Network Access Restriction table, there shouldn't be any reason with the server itself that the ssh wouldn't be working in the SecureSync. External to the SecureSync, make sure that TCP port 22 is open on any firewalls in between and on your PC.

To verify SSH is still enabled in the server, login to the SecureSync's browser and then, navigate to the **Management -> Network** page of the browser. In the lower-left corner, make sure the "SSH" slider switch is set to "ON" (with a green fill). If it's still enabled, I suspect there is a firewall on your PC or between the SecureSync and your PC which is now blocking port 22.

Let me know what you find and then we can go from there!!



**Keith sent to Danny Loke (16 May 13)** Please note that there were no changes to either Radius or SSH (that I'm aware of anyways- I'm double-checking with our Engineers just to be sure) in either the versions 4.8.8 or 4.8.9 software updates.

SSH with Radius login hasn't been available in any version of the SecureSync software. Radius login has always been limited to strictly the web browser (HTTP/HTTPS) login. So your customer wouldn't have been able to login to SSH using the Radius password even before updating the software beyond 4.8.7.

First, SSH has to be enabled in SecureSync in order to be able to use it. Have your customer navigate to the **Network -> General Setup** page of the browser and click on the **"Services"** tab. Make sure SSH Service is set to **"Enabled"**. If it's set to "Disabled, enable it and press Submit.

SSH has specific configurations for login (As configured in the **Network -> HTTPS/SSH Setup** page of the browser, **SSH** tab). The **"SSH Authentication"** field determines if the SSH connection requires no login password- just the correct public key, only a password with no public key, or if it needs either one in order to connect (as shown below):

| Host Keys                  |                       |
|----------------------------|-----------------------|
| Delete Host RSA Key File   | Disabled              |
| Delete Host DSA Key File   | Disabled              |
| Delete Host ECDSA Key File | Disabled              |
| Create Host Key Files      | Disabled              |
| Host Key Status            | Valid RSA, DSA, ECDSA |
| RSA Key Length             | 2048                  |
| DSA Key Length             | 1024                  |
| ECDSA Key Length           | 521                   |

| SSH Authentication  |                        |
|---------------------|------------------------|
| Authentication Type | Public Key or Password |
| Public Keys File    | Public Key or Password |
| View or Edit        | Disabled               |

Have your customer verify the current settings in this page of the SecureSync. At least for test purposes, temporarily set it to "Only Password" so that it can only connect with the proper password. This can be changed later, as desired.

With version 4.8.8 software installed in a SecureSync, I just created two local login accounts, one with user rights and one with admin rights. I was then able to connect to SSH using both of these two accounts with no problems (the rights don't restrict the ability to connect to SSH). If your customer still can't login to SSH with any User accounts, please have them verify that Port 22 is open on any firewalls on the PC or in between the PC and the NTP server.

Please let me know what they find was preventing the SSH connection, so that I know they are all set- Thanks

---

## FTP and SFTP/SCP (Secure Copy Program)

### A) FTP (File Transfer Program)(no longer available in v5.9.3 and above)

- (Aug 2021) FTP has been removed due to being an insecure Service (starting in v5.9.2)

### B) SFTP/SCP (SecureSync Copy Program)

- Refer to online SecureSync user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/SSH\\_Configuration.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm)
  - Select “File Transfer Using SCP and SFTP”

- ▼ **Secure File Transfer Using SCP and SFTP**

SecureSync provides secure file transfer capabilities using the SSH client tools SCP and SFTP. Authentication is performed using either Account Passwords or Public Key with Passphrase.

Example output from OpenSSH, SCP, and SFTP client commands are shown below.

**SFTP/SCP** (Secure Copy Program) is a secure means of copying files from one system to another, using the underlying Secure Shell.

---

## \*\*tcpforwarding (TCP forwarding)

- tcpforwarding is disabled in all software versions

**Email from Paul Myers (15 Jan 2014)**

The SSHD Configuration files have “AllowTcpForwarding no” by default. I think this has been this configuration for some time. It is either the default or I turned it off since the NetClock 93xx. NetClock 93xx has it turned off as well.

---

## User Rights/Permissions

- Permissions / rights are determined by the Group (user or admin) setting of the local account created in the SecureSync.

**“user” group limitations include:**

- Being able to read but not change network settings.
- Being able to read but not change the state of Services (such as telnet,ftp ssh)

If a “user” is logged in with ssh/telnet and they try to perform an admin-only task, “**you must be an administrator to invoke the xxxxx command**” is displayed.

Below, I can view whether or not DHCP is enabled on Eth2, but I cannot change it (because I am a user group member):

Below, I can view the current static IP address of Eth0. but I cannot change it (because I am a user Group member):

```
kwing@Spectracom ~ $ ip4get 0
10.2.100.176/16 S
kwing@Spectracom ~ $ ip4set 0 10.10.10.1 255.255.255.0
You must be an administrator to invoke the ip4set command.
kwing@Spectracom ~ $ █
```



I also mentioned that users cannot change the state of services (such as telnet, ssh, http, etc). Changes to the state of each Service (such as telnet) require an account with admin rights. Below, I can view that telnet is not enabled. But I cannot enable it (because I am a user Group member):

```
ving@Spectracom ~ $ servget 2
telnet Service          disabled
ving@Spectracom ~ $ servset 2 on
you must be an administrator to invoke the servset command.
ving@Spectracom ~ $
```

---

## Security Algorithms (such as RC4)

### **\*\*RC4 (also known as ARC4 or ARCFour)**

- Refer to: <http://en.wikipedia.org/wiki/RC4>
- Refer to Mantis case 2293 [http://cvsmantis.int.oroia.com/mantis/view\\_all\\_bug\\_page.php](http://cvsmantis.int.oroia.com/mantis/view_all_bug_page.php)
- ARCFour consists of ARCFour, ARCFour 128 and ARCFour 256
- ARCFour is known to be weak. ARCFour 128 and ARCFour 256 improve these ciphers by removing the less secure portion of the cipher.
- ARCFour was enabled, but at the bottom of the cipher selection list, in at least version 5.0.0 and below
- ARCFour was disabled in version 5.2.1 update.

Q. We need to disable RC4 for SSH. Can you folks tell me how that can be done?

**A. Reply from Paul Myers to Wade Sober (8 July 2013)**

If SSH users do NOT want RC4, Please have Keith collect the customer requirements and enter a Mantis case.

Does the customer have a security reason why RC4 should be removed?

If it is generally applicable, we can consider removing it for all customers in a subsequent release.

I think this would require rebuilding of OpenSSL or less likely OpenSSH.

I don't recall an OpenSSH configuration operation to disable RC4.

For HTTP there might be such an option but they are referring to SSH correct?

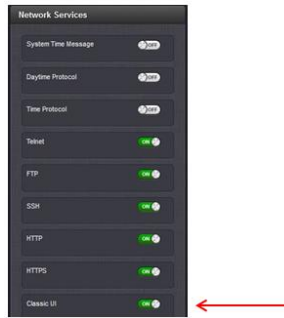
### **Update for questions below:**

- RC4 was initially removed in update version 5.0.1 (Refer to Mantis case 2293)
- RC4 was then brought back into the software with version 5.1.5 (Refer to Mantis case 2918). It is also confirmed to be enabled in versions 5.1.7. 5.1J and 5.2.0 as well. It was added in to help address a vulnerability issue that was more severe.
- RC4 was then removed in version 5.2.1, as it was no longer needed in order to mitigate another vulnerability issue.

**Note:** In at least versions 5.2.1 through 5.3.1, RC4 cipher is only being used with the earlier "classic interface" web browser. It's not used with the newer black/charcoal browser

- If network scanner is detecting RC4 cipher is present, we recommend disabling the classic interface browser and just using the newer browser.

The classic interface web browser on port 8080 can be disabled in the bottom-left corner of the **Management -> Network** page of the newer black browser. It's the last slide switch in the "**Network Services**" list, labeled as "**Classic UI**" (as shown below). Note there is no need to reboot the SecureSync after sliding this switch to the OFF position.



Q. We need to disable RC4 for SSH (in SecureSync). Can you folks tell me how that can be done?

**A. Reply from Paul Myers to Wade Sober (8 July 2013)**

If SSH users do NOT want RC4, Please have Keith collect the customer requirements and enter a Mantis case.

Does the customer have a security reason why RC4 should be removed?

If it is generally applicable, we can consider removing it for all customers in a subsequent release.

I think this would require rebuilding of OpenSSL or less likely OpenSSH.

I don't recall an OpenSSH configuration operation to disable RC4.

For HTTP there might be such an option but they are referring to SSH correct?

**Email from Paul Myers**

It seems like SSH2 is GOOD with ARCFOUR

<http://www.openssh.org/security.html>

OpenSSH was not vulnerable to the RC4 cipher password cracking, replay, or modification attacks. At the time that OpenSSH was started, it was already known that SSH 1 used the RC4 stream cipher completely incorrectly, and thus RC4 support was removed.

[http://linux.die.net/man/5/sshd\\_config](http://linux.die.net/man/5/sshd_config)  
ciphers described here

[http://csce.uark.edu/~kal/info/private/ssh/ch03\\_09.htm](http://csce.uark.edu/~kal/info/private/ssh/ch03_09.htm)  
Restates RC4 is not useable with SSH1

## Services/Processes/daemons which may be running

To check what processes are currently running

- All processes: At the CLI prompt, type **ps -el** <enter> (Note: **ps -elf** provides even more info)
- To see if a particular process (such as SNMPD and SNMPSAD, our sub-agent) is running, type **ps -el | grep snmp** <enter> (where it will list everything with the name typed after "grep)

```
Spectracom spectracom # ps -el | grep snmp
5 S 1001 2923 1 0 80 0 - 1973 poll_s ? 00:00:01 snmpd
5 S 0 2940 1 0 80 0 - 1989 poll_s ? 00:00:00 snmpsad
Spectracom spectracom #
```

**Note:** when the SNMP enable/disable switch is off, both snmpd and snmpsad should be stopped (not listed)

## List of various daemons/services/processes which may be enabled/running in the unit

**Note:** Not all processes in this list below (such as Broadshield for instance) apply to all SecureSyncs- the list of services actually running in each SecureSync is likely to vary from one unit to the next. Also note there may be others not listed below (such as any that were added after this list was compiled, ~June 2018, for instance)

*list below was from Mike Sutton (28 June 2018)*

**Addlocal**...Service to add a remote user (RADIUS or TACACS+) to the system for SSH login.

**Apache2**... HTTPS

**Apache2-cert**... HTTPS security certifications

**Broadshield**...Service to start the Broadshield software option for jamming/spoofing support

**Discmond**... Daemon to monitor disciplining

**Fcron**...Used in Linux to execute periodic command scheduling

**Fcrontab**...Used by Fcron to create tables in Linux

**Fpaneld**...Daemon to run front panel

**Gbe-load**... Service to load the Gigabit Ethernet driver

**Gpsmond**...Daemon to monitor GPS receiver

**Identify**...Start-up script to identify hardware in the system.

## Ipsetd

- Per Ron D (4 June 2019) "**Ipsetd is a process that we developed for setting IP addresses, and should always be running. I am not sure why it isn't running in their 5.8.2 SecureSync, but I downgraded a unit to 5.8.2 and saw that it is running.**"

**Kalarmd**...Daemon for alarm monitoring and messaging.

**Khtd**... Daemon for managing host time system time.

**Khte**... Program that ensures Linux and the Timing system times agree at start up.

**Kmond**...Linux monitoring Daemon

**Kts**...Kramden Timing System (Spectracom, proprietary)

**Ktslogd**...Daemon for monitoring and logging KTS events.

**Local**...Daemon to set up scripts within Linux which are used during boot or shutdown.

**Logd**...Daemon for monitoring and updating logs

**Modules-load**...commands used for loading/unloading modules into or out of the Linux Kernel

**Net.eht0**...Opens eth0 port with defaults.

**Netmond**...Daemon to monitor network traffic and status.

**Netmount**...network startup on boot

**Notifyd**...Daemon which handles notifications

**Ntpmond**...Daemon to monitor Ntp.

**Nwptide**... Service to discover features that are installed on startup

**Nwpple**... Product labeling service

**Pam**... Linux authentication service

**Perfmond**...Daemon to monitor performance

**Pseudod**...Daemon to handle GPS information using pseudo-terminals for Broadshield (now called "SecureSync Interference Detection Suite Option")

**Rexd**...Daemon to monitor other daemons

**Snmprd**...Daemon to monitor and facilitate process SNMP requests and redirect them to subservers (agents), that generate SNMP messages payload. One basic agent is integrated, the other is snmpsad

**Snmpsad**... Daemon to monitor and facilitate SNMP MIB. Traps.

**Sql\_Db**...database for the Web U/I.

**Sshd-create-keys**...Daemon to create SSH keys for console access.

**Statusd**...Daemon to report system status.

**Sysklogd**...Daemon to monitor and report syslog

**Xinetd**...Networking Daemon

---

## Controlling Services as spfactory (internal use only)

**Kill a particular process that is currently running (such as snmpsad from above screenshot)**

- Type: **kill** followed by the **pid number** ("2940" in the above screenshot). Example: **kill 2940** <enter>.

## Start or stop services (such as SNMP, NTP etc)

- 1) Change to /etc/init.d
- 2) Type the name of service (such as **snmpd**) followed by **start** or **stop** or **zap**
- 3) Zap (zap is for stopping a crashed service such as SNMP, NTP etc)
- 4) Change to /etc/init.d
- 5) Type the name of service (such as **snmpd**) followed by **zap**. Example: **snmpd zap**
- 6) Type the name of service (such as **snmpd**) followed by **start**. Example: **snmpd start**

Example **ps -elf** command from a v5.2.1 unit operating normally:

```

spadmin@Spectracom ~$ ps -elf
USER      PID   C  PRI  NI  ADDR  SZ  WCHAN  STATE  TTY          TIME
spadmin   1     0  0    0    0     0     0     S      0:00.00  ?
spadmin   2     0  0    0    0     0     0     S      0:00.00  ?
spadmin   3     0  0    0    0     0     0     S      0:00.00  ?
spadmin   4     2  0    0    0     0     0     S      0:00.00  ?
spadmin   5     2  0    0    0     0     0     S      0:00.00  ?
spadmin   7     2  0    0    0     0     0     S      0:00.00  ?
spadmin   8     2  0    0    0     0     0     S      0:00.00  ?
spadmin   9     2  0    0    0     0     0     S      0:00.00  ?
spadmin  10     2  0    0    0     0     0     S      0:00.00  ?
spadmin  11     2  0    0    0     0     0     S      0:00.00  ?
spadmin  12     2  0    0    0     0     0     S      0:00.00  ?
spadmin  13     2  0    0    0     0     0     S      0:00.00  ?
spadmin  14     2  0    0    0     0     0     S      0:00.00  ?
spadmin  15     2  0    0    0     0     0     S      0:00.00  ?
spadmin  16     2  0    0    0     0     0     S      0:00.00  ?
spadmin  17     2  0    0    0     0     0     S      0:00.00  ?
spadmin  20     2  0    0    0     0     0     S      0:00.00  ?
spadmin  21     2  0    0    0     0     0     S      0:00.00  ?
spadmin  58     2  0    0    0     0     0     S      0:00.00  ?
spadmin  59     2  0    0    0     0     0     S      0:00.00  ?
spadmin  60     2  0    0    0     0     0     S      0:00.00  ?
spadmin  61     2  0    0    0     0     0     S      0:00.00  ?
spadmin  62     2  0    0    0     0     0     S      0:00.00  ?
spadmin  69     2  0    0    0     0     0     S      0:00.00  ?
spadmin  899    1  0    0    0     0     0     S      0:00.00  ?
spadmin 1208    1  0    0    0     0     0     S      0:00.00  ?
spadmin 2022   4288  0  0    0     0     0     S      0:00.00  ?
spadmin 2871    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3041    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3647    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3159    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3161  3159  0  0    0     0     0     S      0:00.00  ?
spadmin 3184    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3215    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3239    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3259    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3279    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3335    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3697    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3847    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3687    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3774    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3976    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3821    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3895    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3933    1  0    0    0     0     0     S      0:00.00  ?
spadmin 3995    1  0    0    0     0     0     S      0:00.00  ?
spadmin 4861    2  0    0    0     0     0     S      0:00.00  ?
spadmin 6064    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6104    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6208    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6554    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6355    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6357    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6358    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6359    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6360    1  0    0    0     0     0     S      0:00.00  ?
spadmin 6270  6208  0  0    0     0     0     S      0:00.00  ?
spadmin 6208  6104  0  0    0     0     0     S      0:00.00  ?
spadmin 1208  3159  0  0    0     0     0     S      0:00.00  ?
spadmin 15214 3770  0  0    0     0     0     S      0:00.00  ?
spadmin 15215 3821  0  0    0     0     0     S      0:00.00  ?
spadmin 15216 15215 1  0    0     0     0     S      0:00.00  ?
spadmin 15217 15215 0  0    0     0     0     S      0:00.00  ?
spadmin 15218 15214 0  0    0     0     0     S      0:00.00  ?
spadmin 15219 15216 0  0    0     0     0     S      0:00.00  ?
spadmin 15220 15215 0  0    0     0     0     S      0:00.00  ?
spadmin 15233 24431 0  0    0     0     0     S      0:00.00  ?
spadmin 15232 3279 0  0    0     0     0     S      0:00.00  ?
spadmin 15792 2 0  0    0     0     0     S      0:00.00  ?
spadmin 22230 1  0    0    0     0     0     S      0:00.00  ?
spadmin 24276 6064 0  0    0     0     0     S      0:00.00  ?
spadmin 24318 23978 0  0    0     0     0     S      0:00.00  ?
spadmin 24318 24318 0  0    0     0     0     S      0:00.00  ?

```

## netstat -tuln | grep :::

```

tcp6      0      0 :::8080          :::*      LISTEN    port 8080 is used for Timekeeper option (if license file installed)
tcp6      0      0 :::80            :::*      LISTEN    port 80 is used for HTTP web U/
tcp6      0      0 :::21            :::*      LISTEN    port 21 is used for FTP

tcp6      0      0 :::22            :::*      LISTEN    port 22 is used for SSH, SCP
tcp6      0      0 :::23            :::*      LISTEN    port 23 is Telnet, unencrypted text communications to the unit
tcp6      0      0 :::443           :::*      LISTEN    port 443 is used for Https, SSL

udp6      0      0 :::57543         :::*
udp6      0      0 :::161           :::*

spadmin@Spectracom ~$

```

In addition to the list above, port 123 is for NTP packets, and port 161 is for SNMP packets

**ss -lntu** command to find a list of all open ports  
refer to L <https://www.tecmint.com/find-open-ports-in-linux/>

## RFCs

The Internet Engineering Task Force website (has a section titled "RFC pages". RFC's (Request For Comments) provide a breakdown of the many protocols used by computers and networks. Refer to <http://www.ietf.org/rfc.html> to query for a specific RFC.

## RFC-1213/ports for the SecureSync

MIB-2 is officially defined in RFC1213. Type in "1213" where it asks for the RFC number. This will give you Management Information Base for Network Management protocol for TCP/IP-based Internets (MIB-II).

For a "complete" list of **ports**, refer to: [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

## UDP/TCP Ports for the SecureSync/9400s

| Protocol   | Port | Description               | Associated service (for listening)                                                         | Notes                                                                                                           |
|------------|------|---------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| TCP or UDP | 13   | Daytime                   | Xinetd (although this will launch daytime upon connection)                                 | Daytime protocol (RFC 867): <a href="https://tools.ietf.org/html/rfc867">https://tools.ietf.org/html/rfc867</a> |
| TCP        | 22   | SCP/SFTP                  | Xinetd (although this will launch sshd upon connection) see example log entry to the right | SSH (Secure Shell)<br>Apr 13 17:37:14 Spectracom xinetd[2383]: START: ssh pid=18927 from=::ffff:10.2.100.52     |
| TCP        | 37   | TIME                      | Xinetd (although this will launch time protocol upon connection)                           | Time protocol (RFC 868): <a href="https://tools.ietf.org/html/rfc868">https://tools.ietf.org/html/rfc868</a>    |
| UDP        | 53   | DNS                       |                                                                                            | <a href="#">Domain Name System</a>                                                                              |
| TCP        | 80   | HTTP                      | HTTP                                                                                       | Optional, if HTTPS is normally used)                                                                            |
| UDP        | 123  | NTPD                      | NTPD                                                                                       | <a href="#">Network Time Protocol</a> (NTP)                                                                     |
| UDP        | 161  | SNMP                      | snmpd                                                                                      | (Factory default is 161, but is user-configurable)                                                              |
| UDP        | 162  | SNMP TRAPS                | snmpd                                                                                      | (Factory default is 162, but is user-configurable)                                                              |
| TCP        | 443  | HTTPS/SSL                 | Apache2                                                                                    | Associated with the Apache browser                                                                              |
| UDP        | 514  | syslog                    | syslogd                                                                                    | <a href="#">Remote Shell</a> , Factory default is port 514. Can be changed in versions 5.7.1 and above,         |
| UDP        | 319  | ptpv2                     | ptpd                                                                                       | PTP protocol                                                                                                    |
| UDP        | 320  | ptpv2                     | ptpd                                                                                       | PTP protocol                                                                                                    |
|            | 8080 | Classic Interface browser |                                                                                            | Classic Interface web browser (when enabled in new browser)                                                     |
|            | 8888 | Timekeeper                |                                                                                            | <i>Timkeeper software option (when enabled) w/license</i>                                                       |

➤ **xinetd** (per <https://en.wikipedia.org/wiki/Xinetd>)

*xinetd listens for incoming requests over a network and launches the appropriate [service](#) for that request.<sup>[9]</sup> Requests are made using [port numbers](#) as identifiers and xinetd usually launches another [daemon](#) to handle the request. It can be used to start services with both privileged and non-privileged port numbers.*

## Network related (network settings/DNS/Port enabling)

### Network Discovery/Network Auto Discovery/Auto-Discovery

- for general info, refer also to associated “Network Discovery” in: <..\CustomerServiceAssistance.pdf>

per <https://www.bing.com/search?q=auto+discover+network&gs=SC&pg=autodiscover+network&sk=AS1&sc=6-20&cvid=E0055639B243408EA04BC4283BC25288&FORM=QBRE&sp=2>

“Based on the **network** location you choose, Windows will **automatically** assign a **network discovery** state to the **network** and opens the appropriate Windows Firewall ports for that state. **Network discovery** is a **network** setting that affects whether your computer can find other computers and devices on the **network** and whether other computers on the **network** can find your computer”

### Specific to Model 1200 SecureSyncs

- Model 1200 SecureSyncs/9400s do not support this capability, as of **at least** versions 5.8.5 and below (at least Sept 2019 and prior)
- Refer to Salesforce cases such as 209596 (requesting it be available in 1200 SecureSync)

Q They need to configure and hide the equipment for ping or scanning (over the network) the other users, for this reason need configure THE ALLOW NETWORK DEVICE DISCOVERY.

**A Keith's response (27 Sept 2019 for at least versions 5.8.6 and below):** This ability is not currently available in the SecureSync. However, I will be happy to forward your customer's desire to have this capability available over to the

SecureSync's Senior Product Manager for his consideration of potentially adding it to the SecureSync, via a future software update

## Management -> Network Setup page (for eth0, eth1, eth2, eth3)

The screenshot displays the Spectracom NetClock 9483 management interface. The top navigation bar includes 'HOME', 'INTERFACES', 'MANAGEMENT', 'TOOLS', 'MONITORING', and 'HELP'. The 'MANAGEMENT' section is active, showing a sidebar with 'Actions' (General Settings, VMO Interface Settings, Access Control, Login Banner, SSH, HTTPS, System Time Message) and 'Network Services' (System Time Message, General Purpose Input Time Stamping, Daytime Protocol, Time Protocol, Telnet, FTP, SSH, HTTP, HTTPS, tcpdump). The main content area shows a 'Ports' table with columns for PORT, ACTION, and STATUS.

| PORT | ACTION        | STATUS                           |
|------|---------------|----------------------------------|
| eth0 | [On/Off/Menu] | CONNECTED (100MB/S, FULL DUPLEX) |
| eth1 | [On/Off/Menu] | CONNECTED (100MB/S, FULL DUPLEX) |
| eth2 | [On/Off/Menu] | DISABLED                         |
| eth3 | [On/Off/Menu] | DISABLED                         |

## Report of *Management* -> *Network Setup* page not displaying eth0 or the GB interfaces (eth1, eth2, eth3)

1. Refer to Case 274942 (the report was for 2400 SecureSync, but same also applies to 1200 SecureSync)
2. Was due to being logged in as a USER account (instead of an admin account). User account doesn't have rights to view or change network settings.

**Reply from Dave Lorah (9 Nov 2021)** The reason you are seeing only the one Icon instead of three on the Network Setup screen is because you are logged in with an account that has only User privileges, which is read only. The configuration Icons are not visible if logged in with a User Account.

You can either login to the spadmin account or change your User Account privileges to Admin instead of User.

The front panel doesn't have a login and is always capable of setting the Network parameters.

## Display network (UDP/TCP) network ports open/Network port assignments (such as port 123 is for NTP)

### Netstat commands

- Refer to netstat section in this doc: [netstat and ss commands](#)
  - "To list all open ports or currently running ports including **TCP** and **UDP** in Linux, we will use [netstat](#), is a powerful tool for monitoring network connections and statistics."

### Available variants of the netstat command

- refer to sites such as: <https://www.tecmint.com/20-netstat-commands-for-linux-network-management/>  
<https://www.tecmint.com/find-open-ports-in-linux/>

To list all open ports or currently running ports including TCP and UDP in Linux, we will use [netstat](#), is a powerful tool for monitoring network connections and statistics.

```
List All Network Ports Using Netstat Command
$ netstat -ltn
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp    0      0 :::22                  :::*                     LISTEN
tcp    0      0 :::80                   :::*                     LISTEN
tcp    0      0 :::25                   :::*                     LISTEN
udp    0      0 0.0.0.0:68              0.0.0.0:*               LISTEN
```

Where,

- `-l` - prints only listening sockets
- `-n` - shows port number
- `-t` - enables listing of tcp ports
- `-u` - enables listing of udp ports

## CLI Command to report port statuses

Per Eric Girard (June 2022) `grep <service name > etc/services` will report each used port for each protocol

```
spadmin@SecureSync ~ $ grep ntp /etc/services
nntp      119/tcp      readnews untp  # Network News Transfer Protocol
nntp      119/udp      readnews untp
ntp       123/tcp      # Network Time Protocol
ntp       123/udp
nntps     563/tcp      snttp      # NNTP over SSL
nntps     563/udp      snttp
trnsprntproxy 3346/tcp    # Transparent Proxy
trnsprntproxy 3346/udp
spadmin@SecureSync ~ $ grep snmp /etc/services
snmp      161/tcp      # Simple Net Mgmt Proto
snmp      161/udp
snmptrap  162/tcp      snmp-trap  # Traps for SNMP
snmptrap  162/udp      snmp-trap
snmp-tcp-port 1994/tcp    # cisco SNMP TCP port
snmp-tcp-port 1994/udp
spadmin@SecureSync ~ $ grep ldap /etc/services
ldap      389/tcp      # Lightweight Directory Access Protocol
ldap      389/udp
ldaps     636/tcp      # LDAP over SSL
ldaps     636/udp
```

---

## “Unexpected” network ports being reported as open/listening

### 1. Port 68 (associated with DHCP/dhclient)

- Refer to Salesforce cases, such as merged Cases 260108/260109 (March 2021)
- Refer to JIRA tickets such as **SSS-392** (Tim Hammer reproduced in **5.8.9** and **5.9.1**)



## \*\*Port speeds/duplex selections

- **Versions 5.7.3 and below:** Can disable Autonegotiation to configure speed and duplex
- **Versions 5.7.2 and below:** hardset to Autonegotiation all interfaces

### (v5.7.3/5.8.0 and above) Added enable/disable link negotiation and ability to hard-set port settings

- Limited distribution Update **v5.7.3** (and general update releases 5.8.0/5.8.1) added capability to enable/disable link auto-negotiation and set individual network port speed/duplex settings
- Applies to all ethernet interfaces (eth0 through eth3)

#### A) Configuring via CLI (**speedget** and **speedset** commands)

- One of the new features in the next firmware release version 5.8.0 is the ability to control the port settings through the **speedset** and **speedget** CLI commands.

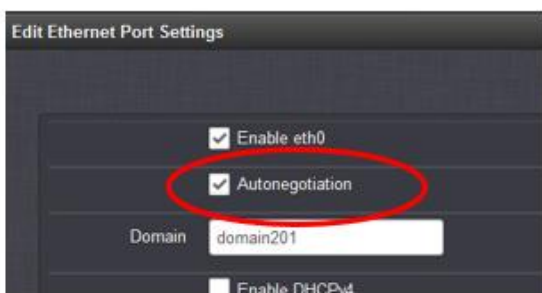
```
spadmin@Spectracom ~ $ speedget
eth0=autoneg on (100Mb/s Full)
eth1=autoneg on (Unknown! Unknown!)
eth2=autoneg on (Unknown! Unknown!)
eth3=autoneg on (Unknown! Unknown!)
spadmin@Spectracom ~ $ speedset
Invalid arguments
Usage: speedset <intfc> <autoneg> (<speed> <duplex>)
      intfc: 0=eth0, 1=eth1, etc.
      autoneg: on|off (provide speed/duplex if autoneg off)
      speed: 10|100|1000
      duplex: full|half
spadmin@Spectracom ~ $
```

#### B) Configuring via web browser

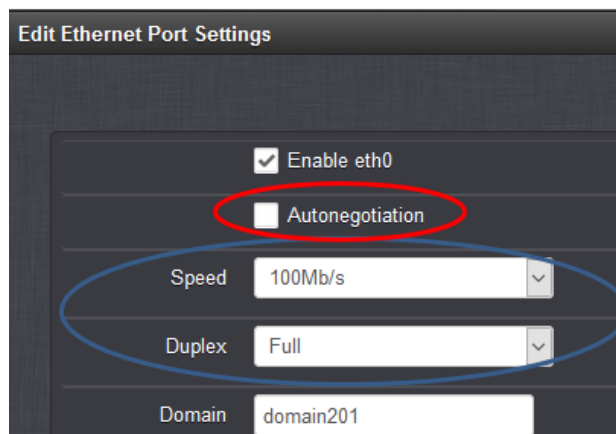
**Management** -> **Network Setup** page,

Click the middle icon (pencil) for each interface (eth0 thru eth3)

“Autonegotiation” enabled (default)



“Autonegotiation” disabled



#### Logging of associated port settings in the kern.log

- Port speeds (such as 10Mbps, 100Mbps or 1000Mbps) and duplex selection (half duplex or full duplex) for the Ethernet interfaces are logged in the kern.log
  - Example kern.log entry: 8139too 0000:00:06:0 eth0: link up, 100Mbps, full-duplex, lpa 0xC101

---

## (Applicable to v5.9.4) periodic eth0 latencies (such as delays in Ping, NTP offset spikes)

- Refer to Salesforce Cases such as 280013
- Refer to JIRA **SSS-1250** (patch now available for v5.9.4). Refer to folder (“**Eth0 Latencies in 5.9.4 patch**”) [\\rocfnp02\idrive\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\](#)
- Hotpatch was implemented in the version 5.9.5 update.
- Periodic latencies (tens of milliseconds, to hundreds of milliseconds) with eth0 only, observed after updating to version 5.9.4 (same as purchasing a new unit with 5.9.4 installed). Results in periodic very long ping response times, NTP timing offset spikes etc, sometimes to around 900 ms.
- Generally associated with the time delay between packets being received on eth0 and the received packets then being processed.

---

## 10/half can cause eth0/ETX lock-ups (versions 5.4.1 and below)

- **Update version 5.4.5** updated the Ethernet “8139too” driver to version 0.9.88 to improve operation of eth0
- This was to fix the issues with eth0 potentially hanging/locking up if the port is set to 10/half (for example, it couldn’t negotiate with its switch).

### Versions 5.4.1 and below

- Switch should be set to auto-negotiate.
- Switches that are hard-set cause Eth0 to go to 10/half
- 10/half in a busy network can cause a watchdog reset of the ETX (indicated in the kernel log):

```
14 16:04:31 Spectracom kernel: -----[ cut here ]-----
Jun 14 16:04:31 Spectracom kernel: WARNING: CPU: 0 PID: 0 at net/sched/sch_generic.c:303
dev_watchdog+0x199/0x1b0()
Jun 14 16:04:31 Spectracom kernel: NETDEV WATCHDOG: eth0 (8139too): transmit queue 0 timed out
Jun 14 16:04:31 Spectracom kernel: Modules linked in: e1000e(O) e100 8139too mii tsyncpci(O)
Jun 14 16:04:31 Spectracom kernel: CPU: 0 PID: 0 Comm: swapper Tainted: G      O  4.0.5-gentoo #1
Jun 14 16:04:31 Spectracom kernel: Hardware name: /AMD-GX3, BIOS 6.00 PG 11/04/2008
Jun 14 16:04:31 Spectracom kernel: dec09f58 dec09f58 dec09f2c c133d015 dec09f48 c10330c5 0000012f c128ab49
Jun 14 16:04:31 Spectracom kernel: dee66000 00000000 ffff88a dec09f60 c1033116 00000009 dec09f58 c141d664
Jun 14 16:04:31 Spectracom kernel: dec09f74 dec09f94 c128ab49 c1419d6e 0000012f c141d664 dee66000
e082fa9c
Jun 14 16:04:31 Spectracom kernel: Call Trace:
Jun 14 16:04:31 Spectracom kernel: [<c133d015>] dump_stack+0x16/0x18
Jun 14 16:04:31 Spectracom kernel: [<c10330c5>] warn_slowpath_common+0x65/0x90
Jun 14 16:04:31 Spectracom kernel: [<c128ab49>] ? dev_watchdog+0x199/0x1b0
Jun 14 16:04:31 Spectracom kernel: [<c1033116>] warn_slowpath_fmt+0x26/0x30
Jun 14 16:04:31 Spectracom kernel: [<c128ab49>] dev_watchdog+0x199/0x1b0
Jun 14 16:04:31 Spectracom kernel: [<c128a9b0>] ? dev_graft_qdisc+0x60/0x60
Jun 14 16:04:31 Spectracom kernel: [<c105bb21>] call_timer_fn.isra.42+0x11/0x70
Jun 14 16:04:31 Spectracom kernel: [<c105bd36>] run_timer_softirq+0x126/0x1a0
Jun 14 16:04:31 Spectracom kernel: [<c1035661>] __do_softirq+0xc1/0x1a0
Jun 14 16:04:31 Spectracom kernel: [<c10355a0>] ? __tasklet_schedule+0x40/0x40
Jun 14 16:04:31 Spectracom kernel: [<c10037ec>] do_softirq_own_stack+0x1c/0x30
Jun 14 16:04:31 Spectracom kernel: <IRQ> [<c1035815>] irq_exit+0x45/0x50
Jun 14 16:04:31 Spectracom kernel: [<c10035cd>] do_IRQ+0x3d/0xb0
Jun 14 16:04:31 Spectracom kernel: [<c134042c>] common_interrupt+0x2c/0x34
Jun 14 16:04:31 Spectracom kernel: [<c1008855>] ? default_idle+0x5/0x10
Jun 14 16:04:31 Spectracom kernel: [<c1009009>] arch_cpu_idle+0x9/0x10
Jun 14 16:04:31 Spectracom kernel: [<c105002e>] cpu_startup_entry+0x20e/0x2a0
```

```
Jun 14 16:04:31 Spectracom kernel: [<c133c017>] rest_init+0x57/0x60
Jun 14 16:04:31 Spectracom kernel: [<c14899f9>] start_kernel+0x2fa/0x2ff
Jun 14 16:04:31 Spectracom kernel: [<c14892b3>] i386_start_kernel+0x81/0x85
Jun 14 16:04:31 Spectracom kernel: ---[ end trace f4120b60010b3291 ]---
Jun 14 16:04:34 Spectracom kernel: 8139too 0000:00:06.0 eth0: link up, 10Mbps, half-duplex, lpa 0x0000
```

---

## Unit lockups and no/Losses of network connectivity between eth0 and a switch/unless both devices are hard-set (instead of auto-negotiate)

- Refer to case 212522
- Could only Good Link/network connectivity once eth0 and the switch being hard-set to 100/full
- customer moved to one of the 1204-06 interfaces which fixed it.

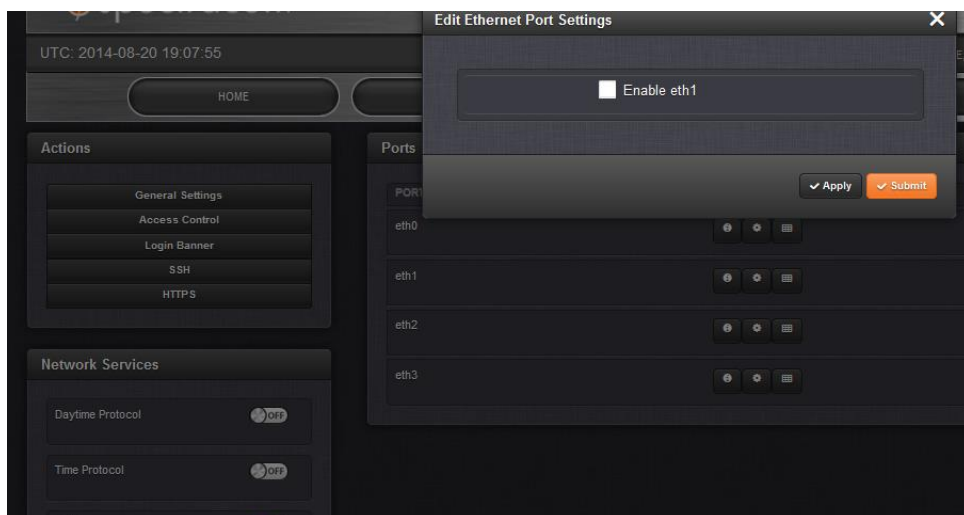
---

## \*\*Desire to Enable/Disable the Gigabit interfaces (eth1, eth2 and/or eth3)

- The ability to enable or disable gigabit ports eth1, eth2 and/or eth3 started in Archive version 5.1.2 (first release of the new web browser design).
- Ethernet interfaces cannot be disabled with the “classic view” (original) web browser in versions 5.0.2 and below. Must be enabled/disabled using newer web browser.

### A) Enable/disable the Ethernet interfaces via the web browser

- 1) **Management** -> **Network** page of the browser
- 2) Click on the center “**GEAR**” ICON (center of the three ICONS) to open the pop-up window.
- 3) Select the “**Enable eth**” checkbox to expand the pop-up window.
- 4) Configure the port settings as desired (unselect **DHCP** to configure a static address).



### B) CLI command to enable/disable the Gigabit ports

- The CLI command: **portset x on** enables the interface number specified by the “x”.
- The CLI command: **portset x off** disables the interface number specified by the “x”

**C) Enable/disable the Ethernet interfaces via the front panel keypad/LCD display (available in versions 5.6.0 and above)**

- Refer to (in this doc): [Configure/display network settings using keypad](#)

**To enable each interface via the front panel keypad:**

1. First press the ✓ key to go into the initial setup menu.
2. Then use the white arrow keys to highlight (and then the ✓ key to select) the main “netv4” menu.
3. In the next menu, use the white arrow keys to highlight (and then the ✓ key to select) the Ethernet interface you wish to enable (such as “eth1” for instance)
4. Then highlight/select “Port”
5. The next menu is all set to perform the opposite of its current state (with it currently disabled, it’s all set to be enabled for instance). Just press the ✓ key to select the change and then press the same key again to apply this change. A few moments later, the port will be enabled and ready to be configured.

FYI: After enabling each interface, it can be configured via the front panel using the other sub-menus under the “netv4” menu. For a static address, first disable DHCP via the DHCP menu. Then configure the IP address via the IP Addr sub-menu, etc,

**Issue with 5.1.2: Not able to disable a port (Eth1, Eth2 or Eth3) once it's been enabled.**

- Version 5.1.2 doesn't allow you to disable again a port that has been enabled.
- Refer to Mantis case 2754 <http://cvsmantis.int.rolia.com/mantis/view.php?id=2754>

Q I was working on trying to disable a port and it would not let me submit the “edit Ethernet port settings” with the enable ethx after I had set it up as a working port it kept giving an error and would not disable the port.

**A (reply from Dave Lorah)** I attempted to duplicate it and I see the same thing. This appears to be a bug in the new firmware and we are investigating.

The port can be enabled or disabled via telnet or serial interface. Use the portget command to view the port state. The portset X (on or off) command will enable or disable the individual port where X is 0,1,2 or 3 for the port number. Example: “portset 1 off” disables Ethernet port eth1.

At this time, this is the only way to disable the port after it has been enabled.

**Full Example of enabling and configuration of eth1 via CLI interface**

Note that it's much easier to configure network settings via the CLI (ssh session) as the browser refreshes/delays can be “misleading” (such as trying to make a change while it's still disabling DHCP in the background. for instance).

Please perform the following steps to configure Ethernet interface eth1 as you desire, using ssh. Then, once the settings have been applied, use the web browser to confirm all the settings of eth1 have been successfully applied.

After logging into the cli with an ssh session:

- 1) Type **portset 1 on**<enter> (to enable the port)
- 2) Type **net4 1**<enter> (to display the current settings of eth

```
spadmin@Spectracom ~ $ net4 1
Spectracom
eth1 (Unplugged)
00:0c:ec:05:04:4e
71.44.37.103/25 S
DG4=0.0.0.0
```

- 3) Type **dhcp4get 1**<enter> (make sure it returns “Disabled”)

```
spadmin@Spectracom ~ $ dhcp4get 1
DHCPv4 (eth1)=Disabled
```

- 4) Type **ip4set 1 71.44.37.103 255.255.255.128**<enter> Several seconds later the command prompt will be available again

```
DHCPv4 (eth1)=Disabled
spadmin@Spectracom ~ $ ip4set 1 71.44.37.103 255.255.255.128
```

- 5) Type **gw4set 1 71.44.37.126**<enter> Several seconds later the command prompt will be available again

```
spadmin@Spectracom ~ $ dns4set 1 71.44.34.10 71.44.38.10
spadmin@Spectracom ~ $
```

- 6) Type **dns4set 1 71.44.34.10 71.44.38.10**<enter> Several seconds later the command prompt will be available again

```
spadmin@Spectracom ~ $ dns4set 1 71.44.34.10 71.44.38.10
spadmin@Spectracom ~ $
```

- 7) After several seconds, type again **net4 1**<enter> (to display the current settings of eth1), Confirm the eth3 is now configured as you desire them:

```
spadmin@Spectracom ~ $ net4 1
Spectracom
eth1 (Unplugged)
00:0c:ec:05:04:4e
71.44.37.103/25 $
DG4=71.44.37.126
DNS1:71.44.34.10
DNS2:71.44.38.10
DHCPv4 (eth1)=Disabled
spadmin@Spectracom ~ $
```

- 8) Now log into the web browser and navigate to the network settings, to verify Eth1 settings are being displayed, as you desire them:

The screenshot shows a network configuration interface with the following fields and values:

- Enable DHCPv4
- Static IPv4 Address: 71.44.37.103
- Network: 255.255.255.128
- IPv4 Gateway: 71.44.37.126
- DNS Primary: 71.44.34.10
- DNS Secondary: 71.44.38.10
- Enable DHCPv6
- Enable SLAAC
- IPv6 Gateway: [empty]
- MTU: 1500 [dropdown]

## \*\*Desire to display port state of all Ethernet ports (port up, port down, cable unplugged)

- CLI command is **portstate**
- Displays status of all installed Ethernet ports, including Eth0

```
spadmin@Spectracom ~ $ portstate
eth0=Up
eth1=Unplugged
eth2=Unplugged
eth3=Unplugged
```

### Ethernet port states via SNMPGets

Note that in addition to the port states being available via the **portstate** CLI command, they are also available via SNMPGets in the generic (not Spectracom-specific) RFC-1213 MIB. The name of the object for the states of each port in the RFC1213 MIB is **ifOperStatus** (as shown below):

The **ifDescr** object lists all of the available interfaces in the time server and reports the “assigned name” for each one.

|                     |  |
|---------------------|--|
| <b>ifOperStatus</b> |  |
| . ifLastChange      |  |
| . ifInOctets        |  |
| . ifInUcastPkts     |  |
| . ifInNUcastPkts    |  |
| . ifInDiscards      |  |
| . ifInErrors        |  |
| . ifInUnknownProtos |  |
| . ifOutOctets       |  |
| . ifOutUcastPkts    |  |
| . ifOutNUcastPkts   |  |
| . ifOutDiscards     |  |
| . ifOutErrors       |  |
| . ifOutQLen         |  |
| . ifSpecific        |  |

|                                            |         |
|--------------------------------------------|---------|
| Sent GET request to 10.2.100.176 : 161     |         |
| <b>ifDescr.1</b>                           | lo      |
| <b>ifDescr.2</b>                           | tunl0   |
| <b>ifDescr.3</b>                           | sit0    |
| <b>ifDescr.4</b>                           | ip6tnl0 |
| <b>ifDescr.5</b>                           | eth0    |
| <b>ifDescr.6</b>                           | eth1    |
| <b>ifDescr.7</b>                           | eth2    |
| <b>ifDescr.8</b>                           | eth3    |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.1</b>                      | up(1)   |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.2</b>                      | down(2) |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.3</b>                      | down(2) |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.4</b>                      | down(2) |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.5</b>                      | up(1)   |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.6</b>                      | up(1)   |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.7</b>                      | down(2) |
| Sent GETNEXT request to 10.2.100.176 : 161 |         |
| <b>ifOperStatus.8</b>                      | down(2) |

## DNS servers settings (Primary and Secondary DNS servers)

### Configuration ("etc/resolv.conf" file)

```
[admin@fsm171 etc]$ cat resolv.conf
nameserver 10.1.1.20
nameserver 10.1.1.31
[admin@fsm171 etc]$
```

- Users do not have permission to edit resolv.conf file directly.
- The two DNS Server fields are only displayed in the browser if DHCP is disabled (they are hidden when DHCP is enabled)
- DNS settings should be automatically configured if the port is configured as DHCP enabled
- Manual configuration if DHCP is disabled on that Ethernet interface
- For detailed info on the etc/resolv.conf file, refer to <http://man7.org/linux/man-pages/man5/resolv.conf.5.html>

### A) Via CLI command

#### Display/retrieve/set DNS settings for each Ethernet interface

- The CLI command: **dns4get x** retrieves the DNS setting (for the port specified by the "x").

```
spadmin@Spectracom ~ $ dns4get 1
No Domain Name Servers were found
spadmin@Spectracom ~ $
```

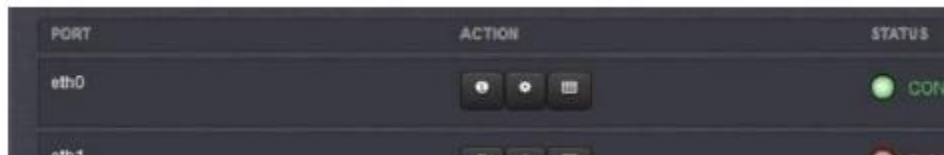
- The CLI command: **dns4set x <primary dns> <secondary dns>** configures the DNS setting for the Ethernet interface port number specified by the "x". (note the second dns address is optional/not required)

```
spadmin@Spectracom ~ $ dns4set 1 10.1.2.3
spadmin@Spectracom ~ $ dns4get 1
DNS1:10.1.2.3
spadmin@Spectracom ~ $ dns4set 1 10.1.2.3 10.4.5.6
spadmin@Spectracom ~ $ dns4get 1
DNS1:10.1.2.3
DNS2:10.4.5.6
spadmin@Spectracom ~ $
```

### B) Via New browser (Management -> Network page of the browser)

**Email from Keith (25 Jun 15)** FYI- the only reason you should have to configure DNS servers is if you are using static network settings. If you are using DHCP, the DHCP server should have configured these settings for you.

For static network settings, the DNS settings are located in the **Management -> Network** page of the web browser. Then click on the middle of the three icons (the gear icon) for the Ethernet interface that you wish to configure.



With the Ethernet interface enabled (top of the pop-up window) and as long as the "Enable DHCPv4" checkbox is not selected, you will see the DNS server fields (these fields are not displayed if the "Enable DHCPv4" checkbox is selected) as shown below:



Available CLI (“dig”) command to help troubleshoot DNS issues

Note (24 Jan KW) Appears dig may have removed (or disabled for spadmin)

### dig: (Domain Information Groper)

- At the command prompt. type “**dig**”

**Function:** a flexible tool for interrogating **DNS name servers**. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

```
1 10.2.100.35 <10.2.100.35> 1.275 ms 0.326 ms 0.268 ms
spadmin@SpectraCom ~1$ dig 10.2.100.35

<<>> DiG 9.4.1-P1 <<>> 10.2.100.35
; global options: printcmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 27049
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

; QUESTION SECTION:
10.2.100.35.                IN      A

; AUTHORITY SECTION:
n-grs.com. 2012042001 1800 900 604800 86400      a.root-servers.net. nstld.verisign

; Query time: 120 msec
; SERVER: 10.1.1.30#53<10.1.1.30>
; WHEN: Fri Apr 20 18:29:31 2012
; MSG SIZE rcvd: 104

spadmin@SpectraCom ~1$
```



## \*\*DNS Host name/ Fully Qualified Domain Name (FQDN)/ (hostname/host name)

**Notice about using DNS host names:** When listing DNS hostnames (instead of IP addresses) to peer NTP servers together, the FQDN (Fully Qualified Domain Name) may need to be used, especially when the devices are not on the same domain.

**Rules for hostnames in linux (Refer to RFCs 952 <https://tools.ietf.org/html/rfc952> and Section 2 of RFC 1123: <https://tools.ietf.org/html/rfc112>)**

A "name" (Net, Host, Gateway, or Domain name) is a text string up to 24 characters drawn from the alphabet (A-Z), digits (0-9), minus sign (-), and period (.). Note that periods are only allowed when they serve to delimit components of "domain style names". (See [RFC-921](https://tools.ietf.org/html/rfc921), "Domain Name System Implementation Schedule", for background). No blank or space characters are permitted as part of a name. No distinction is made between upper and lower case.

The first character must be an alpha character. The last character must not be a minus sign or period. A host which serves as a GATEWAY should have "-GATEWAY" or "-GW" as part of its name. Hosts which do not serve as Internet gateways should not use "-GATEWAY" and "-GW" as part of their names. A host which is a TAC should have "-TAC" as the last part of its host name, if it is a DoD host. Single character names or nicknames are not allowed.

### DNS (Domain Name Storage)

- The domain name for each Ethernet port is stored in the associated "dhclient-eth" config file located in the /etc file (for example, the IPv4 domain name for eth0 is stored in the dhclient-eth0.conf file)

```
spfactory@spectracom /etc $ cat dhclient-eth0.conf
# /etc/dhclient-eth0.conf

interface "eth0" {
    timeout 5;
    retry 10;
    require subnet-mask;
    reject 0.0.0.0/1, 128.0.0.0/1;
}

lease {
    interface "eth0";
    fixed-address 10.2.100.177;
    option subnet-mask 255.255.0.0;
    #option domain-name-servers;
    option domain-name "domain201";
    option routers 10.2.1.1;
    renew 0 2030/1/1 12:00:00;
    rebind 0 2030/1/1 12:00:00;
    expire 0 2030/1/1 12:00:00;
}
```

- If NTP peering isn't working when using hostnames, may need to use FQDN (Fully Qualified Domain Name). Or, setup the domain name on the network interface setup page of the time server for each port, which should allow the single name rather than needing to use the FQDN.

### SecureSync/9400s support just ONE Domain name per Ethernet interface (can't list more than one)

- As of least version 5.6.0 (Apr, 2017), can't list more than one domain name per Ethernet interface.
- Q We were adding some additional domains under below location. We tried adding domains separated by comma, space, semicolon but received error "Invalid domain name"

Management -> Network Setup -> Go to "eth\*" interface -> Click on gear box -> Under domain field add domains < ofi.com ny.ofi.com den.ofi.com tri.ofi.com roc.ofi.com oppenheimerfunds.com >

**A Reply from Dave L (14 Mar 17)** These parameters are limited in the Securesync configuration. The Securesync cannot have more than one Domain name per Ethernet port. Each port can have up to two DNS server addresses.

## Configuration of hostnames

### Factory default hostnames

- **Eth0**: domain201
- **Eth1**: domain202
- **Eth2**: domain203
- **Eth3**: domain204

### Via web browser

#### A) Newer web browser: *Management* -> *Network* page, General Settings button on the left

- To view the current value: click on the left of the three icons (i) for the particular port
- To change the current value: click on the middle of the three icons (gear icon) for the particular port. It's the "Domain" field.



#### Newer browser interface only:

##### SecureSyms/9400s accept:

- Over 40 total characters total in length (not sure exact limit)
- First character can be any number or letter (lower or upper-case)
- Hyphens/minus sign (-) (except as the first character)
- Dots "." (except as the first character)

**Note (about dots):** In order to use any dots in the hostname, it can only be entered via the newer browser. The classic interface doesn't accept any dots.

##### Does not accept:

- Can't be left blank.
- Spaces in the name. However, you can you a hyphen ("-") in place of the space. Note that you cannot use an underscore ("\_") in between.
- Does NOT accept as first or any other character: either parenthesis sign (either "(" or ")") the "and" sign (&) or quote mark ("), colon (:), apostrophe ('), or semicolon (;) or backslash (\), or pound sign ("#") or a plus sign (+), asterisk (\*), underscore ( \_ ), percent sign (%), tilde (~), question mark (?), ampersand (@), (^) exclamation (!), brackets ([ or ]) or { } or { }, or comma (,) forward slash (/)
- Does not accept less than or greater than signs (< or >) anywhere in the string.
- Does not accept dollar sign (random numbers may be returned in its place).

#### B) Classic Interface:

➤ **Network** -> **General Setup** page of the browser, "**General**" tab.

Network-> Interfaces page of the browser (there is a separate tab for each Network interface). It's the "Domain" Field under "Domain Setup".

**Email Keith sent to this customer (15 Nov 2013)** So you are aware, you can define the FQDN in the SecureSync, so that you should be able to use just the single name rather than the FQDN, if you wish. Configure the FQDN in the **Network**-> **Interfaces** page of the browser (there is a separate tab for each Network interface).

The image contains two screenshots of a network configuration web interface. The top screenshot shows the 'Domain Setup' section with fields for DNS Servers (Primary: 10.1.1.20, Secondary: 10.1.1.31) and a Domain field containing 'mt.croha.com'. The bottom screenshot shows the 'NETWORK SETUP' page with tabs for 'General', 'Services', 'Access', and 'Banner'. The 'General' tab is active, showing fields for Hostname (Spectracom), IPv4 Default Gateway Association (eth0), and IPv6 Default Gateway (10.2.1.1). A red arrow points from the 'General' tab to the 'Hostnames' section.

### Accepts:

- Up to 30 total characters total in length.
- First letter can be any number or letter (lower or upper-case)
- First (or any other character in the string, including the last character) can be a plus sign (+), minus sign (-), asterisk (\*), underscore ( \_ ), hyphen (-), percent sign (%), tilde (~), question mark (?), ampersand (@), (^) exclamation (!), Colon (:), brackets ([ or ]) or ({} or {}), or comma (,) forward slash (/)

**Note (about dots):** in order to use any dots in the hostname, it can only be entered via the **newer** browser. The classic interface **doesn't accept** any dots.

### Does not accept:

- Does not accept any dots (.)
- Can't be blank. Will reject the change if you try to delete all characters.
- Spaces in the name (However, you can use an underscore (" \_ ") in place of the space).
- Does NOT accept either parenthesis sign (either "(" or ")") the "and" sign (&) or quote mark ("), semi-colon (;), apostrophe ('), or semicolon (;) or backslash (\).
- Does not accept pound sign (#) as the first character (or the only character). However, it can be any other character in the string, including the last character).
- Does not accept one or more asterisks (\*) by itself without any other characters in the string.
- Does not accept less than or greater than signs (< or >) anywhere in the string.
- Does not accept dollar sign (random numbers may be returned in its place).

## The Link-Local Multicast Name Resolution (LLMNR)

- Refer to Salesforce Case 301047 (for a 1200 but info likely applies to 2400s)
- Refer to [https://en.wikipedia.org/wiki/Link-Local\\_Multicast\\_Name\\_Resolution#:~:text=The%20Link%2DLocal%20Multicast%20Name,on%20the%20same%20local%20link](https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution#:~:text=The%20Link%2DLocal%20Multicast%20Name,on%20the%20same%20local%20link)

“The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.”

### Known issues with the hostname

#### 1. DNS hostname won't accept dashes or capital letters in at least version 5.1.2

- Refer to Mantis case 2737 [http://cvsmantis.int.rolia.com/mantis/view\\_all\\_bug\\_page.php](http://cvsmantis.int.rolia.com/mantis/view_all_bug_page.php)

#### 2. DNS hostname change doesn't take effect until after rebooting the time server.

- With at least versions 4.8.7 and below, a change to the hostname doesn't take effect until the next reboot

---

## Troubleshooting NTP peering

- Use the **Status** -> **NTP** page and NTP log entries to help troubleshoot
- When using hostname to define other NTP servers:
  - A) If they SSH or telnet to the SecureSync, can they ping the hostname of the other NTP server from the command line?
  - B) If just the single name of the hostname (example "spectracom") has the full domain name been configured in the Interfaces page of the browser? This will need to be done.
  - C) Are the other NTP servers on the same domain? If not, the FQDN (not just the single name) will need to be used.

---

## \*\*ARPS / ARP CACHING

**Issue:** ARP messages keep going out around every 35 seconds. (Acts like arp caching issue - not able to store the arps properly).

- Refer to Salesforce case 11297 (<https://na8.salesforce.com/500C000000TDnFi>)
- Paul Myers said this is likely due to adding NTP peers or NTP servers, and this NTP server can't find one or more of the NTP servers on the network due to network or routing issue. So it keeps sending ARP messages to find it.

---

## \*\*TCP connection/TCP session timeouts

**Note:** To see the timeout value, as any user, type "**cat /proc/sys/net/ipv4/tcp\_keepalive\_time**"

- **Factory default TCP timeout is 7200** seconds (as verified in versions 5.2.1, 5.3.1 and 5.4.1)
  - **Factory default TCP timeout is 7200** seconds (with at least versions 4.8.9 and below).
- I entered Mantis case 2060 to make this timeout value user-configurable (as requested by Joel Polleta with Northrop Grumman). Refer to Salesforce Case 10072 for more info

### References for TCP User Timeout:

The relevant standards are:

- <http://tools.ietf.org/html/rfc5482>
- <http://tools.ietf.org/html/rfc793>

**Note:** this info doesn't appear to apply to SSH (or at least SSH in Gentoo-versions 5.0.0 and above anyways)

In at least versions 5.3.1 and below, the TCP timeout value is hard-coded and can't be edited by a user.

Email from Paul Myers

**SHORT ANSWER:**

The default value is 7200 seconds

To see as any user type "**cat /proc/sys/net/ipv4/tcp\_keepalive\_time** " from the command line.

We could control the value via software if we so chose.

**LONG ANSWER WITH THEORY BELOW:**

In regards to the TCP User Timeout

The relevant standards are:

<http://tools.ietf.org/html/rfc5482>

<http://tools.ietf.org/html/rfc793>

How to change:

<http://stackoverflow.com/questions/15484906/change-the-tcp-timeout-for-a-linux-network-device>

<http://www.cyberciti.biz/tips/linux-increasing-or-decreasing-tcp-sockets-timeouts.html>

Excerpted from above link: (Credit given)

Some time it is necessary to increase or decrease timeouts on TCP sockets. You can use `/proc/sys/net/ipv4/tcp_keepalive_time` to setup new value.

The number of seconds a connection needs to be idle before TCP begins sending out keep-alive probes. Keep-alives are only sent when the `SO_KEEPALIVE` socket option is enabled. The default value is 7200 seconds (2 hours).

For example set value to 2400 seconds:

```
echo 2400 > /proc/sys/net/ipv4/tcp_keepalive_time
```

You can make changes to /proc filesystem permanently using `/etc/sysctl.conf`

## Half-Open TCP sessions

- From wikipedia The term half-open refers to [TCP](#) connections whose state is out of synchronization between the two communicating hosts, possibly due to a crash of one side. A connection which is in the process of being established is also known as embryonic connection. The lack of synchronization could be due to [malicious intent](#).
- Both questions below were regarding Salesforce case 16300

Q. Does the SecureSync network stack drop half open TCP sessions after a timeout period? If so, what is the timeout? Is it adjustable?

**A. Keith's response (from Dave Sohn, 30 Oct 2014):** Yes, after ~3 minutes. It is not currently adjustable.

Q. Does the SecureSync network stack set a limit as to the maximum number of half-open TCP sessions allowed? If so, what is the limit?

**A. Keith's response (from Dave Sohn, 30 Oct 2014):** Yes, 128 half-open connections.

---

## \*\* Network Isolation/Network security/FIPS compliancy

### A) General info on network isolation between the SecureSync's interfaces/network ports (eth0, eth1, eth2 and eth3)

- Refer to "1204-06 Gb Ethernet Option Card" section in: <..\SecureSync Option Card information.pdf>
- 1) **Software Issue:** SecureSync with s 1204-06 card installed is "acting like a Hub" (packets sent to one interface are being returned may be returned on a different interface). This was due to "Reverse Path forwarding" ("RP") changes which had been made in the kernel
  - As reported in Salesfoce cases **178238** and **180405**.
  - in software versions such as 5.8.2, 5.8.1 or 5.8.0
  - for details, Refer to the "1204-06 Gb Ethernet Option Card" section in: <..\SecureSync Option Card information.pdf>

### B) FIPS Compliancy (FIPS 140-2)

- For info on FIPS, refer to:
  - [FIPS compliancy \(FIPS 140-2\)](#) (in this document)
  - FIPS (in <..\CustomerServiceAssistance.pdf>)
- Q. Email from Jeremy Thomas (10/13/11) "They site CSG security accreditation (EL4 and above) no doubt we have similar US alternatives"  
**A. Reply from Dave Sohn:** We don't have any security accreditations for the SecureSync
- Q. Email from Jeremy Thomas (10/13/11): The question is the separation and security of SecureSync network timing signals as each test room must ensure absolute security  
**A. Reply from Dave Sohn:** Network isolation is handled within the SW via routing tables and rules.

### HSTS (HTTP Strict Transport Security)

- Refer to "[HTTP / HSTS \(HTTP Strict Transport Security\)](#)" in this document

---

## \*\*\*IEEE 802.3

- Refer to [http://en.wikipedia.org/wiki/IEEE\\_802.3](http://en.wikipedia.org/wiki/IEEE_802.3)
- IEEE 802.3 is a working group and a collection of IEEE standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet.

### IEEE 802.3ad/ IEEE 802.1ax (Link Aggregation Control Protocol"- LACP)

- Link aggregation is a computer networking term to describe various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fail.
  - 802.1ax (back in 2008)
  - 802.3ad (initial release back in 2000)

- Refer to [http://en.wikipedia.org/wiki/Link\\_aggregation#Initial\\_release\\_802.3ad\\_in\\_2000](http://en.wikipedia.org/wiki/Link_aggregation#Initial_release_802.3ad_in_2000)
- As of at least software version 5.5.0 software, SecureSync is not 802.3ad or 802.1ax compliant

## \*\*USB connector/ Ethernet port (eth0- eth3) status LEDs / configuration

### USB connector on rear panel

- I wanted to confirm that the USB port on the rear of the receiver is not enabled. In the users manual it says reserved for future expansion.

**A. Reply from Sam Otto (2 Apr 2013)** Correct, At this time the USB port on the rear of the receiver is not enabled.

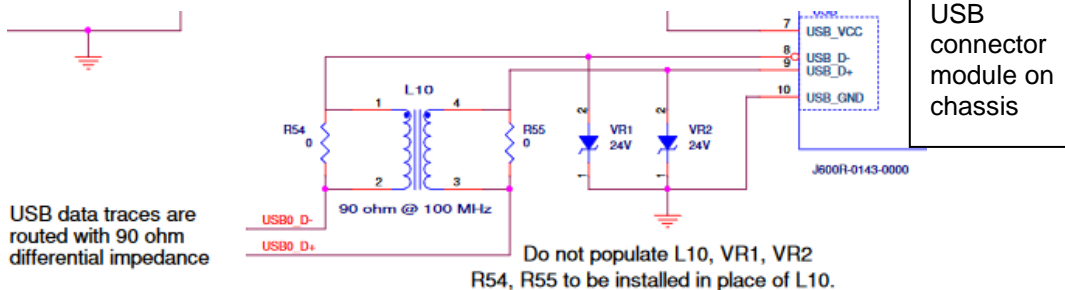
Q The USB Port on the back. I'd like to disable it. Any bright ideas? You appear to have locked down the file structure except via the GUI and this is another thing the GUI doesn't address

**A Keith's response (input from Paul M, 11 Apr 18):** It is already disabled! You can't mount a drive, hardware may provide power. It is NOT mountable and disabled in the operating system.

Q I am also curious and nosy. Is the USB port on the back of the NTP Server so you can hook up a keyboard and break into single-user mode like they used to do with Solaris?

**A Keith's response (input from Paul M, 11 Apr 18):** It is reserved for potential future use only. At this time, the Operating system does NOT include any USB drivers. The power is detectable only. There is no way to mount or use any USB storage or device.

### Excerpt from main board PCB (1200-1001-0200). Do not release





---

## IP address configuration/Ipsetd

### Ipsetd

- Per Ron D (4 June 2019) “Ipsetd is a process that we developed for setting IP addresses, and should always be unning. I am not sure why it isn’t running in their 5.8.2 SecureSync, but I downgraded a unit to 5.8.2 and saw that it is running.”

---

## DHCPv4/DHCPv6

- **Known issue:** Per the v5.9.0 update Release Notes: “DHCPv6 subnet prefixes are currently limited to 64.”

---

## DHClient (“Static lease” default IP addresses for the Ethernet interfaces)

- Assigned “Static” IP addresses are actually “static lease” dynamic address
- Note: The NTP server’s default subnet mask is “16” (255.255.0.0) Not 255.255.255.0. Since 255.255.255.0 is fairly common, a PC directly connected to the network ports may need to be reconfigured as 255.255.0.0 to allow a connection.

| Ethernet port | default “static lease” IP address |
|---------------|-----------------------------------|
| ETH0          | 10.10.201.1                       |
| ETH1          | 10.10.201.2                       |
| ETH2          | 10.10.201.3                       |
| ETH3          | 10.10.201.4                       |

|                                       |
|---------------------------------------|
| <b>Default Subnet:</b><br>255.255.0.0 |
|---------------------------------------|

### Email from Mark Goodlein to Morgan Stanley (7/11/12)

The product may have up to 4 interfaces, each of which may be configured differently (with or without DHCP) but must share some of the same network configuration files (eg. resolv.conf). Because of this, we utilize dhclient for interfaces regardless of whether they are configured for DHCP or static. Each interface has a dhclient.conf file that contains a “static lease” for that interface, which specifies the IP address, mask, DNS servers, domain, etc. When the static parameters are configured on the Web UI or from the command line, they are written into this saved in the static lease in the config file.

When dhclient is invoked to obtain or renew a lease, it will broadcast a request then wait for a response. If no acceptable response is received before some timeout (10 seconds), it will default to using the static lease from the config file. When you configure an interface to be ‘static’ on the SecureSync, what this does is it modifies the dhclient configuration file for that interface by telling it to reject responses to its dhcp request that come from any IP address. This forces dhclient to timeout and use the static lease. When DHCP is ‘enabled’ the interface is configured to allow DHCP responses and it will accept the first valid response it receives from a DHCP server.

When a new DHCP lease is used, a script is run which re-creates the resolv.conf file, pulling together all the domains and DNS servers from each interface. Note: that because we allow 2 DNS servers per interface and may have 4 interface, our system has been modified to support a maximum of 8 DNS servers, instead of the default 3.

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

### UDP port 68 being open (not being able to be closed)

- Refer to Salesforce Case 260108

*On NTP sever (Spectracom Securesync) we noticed that udp port 68 is open (we configured all eth ports to use static IP addresses, DHCP disabled). Is there a way to configure the NTP server (from GUI or command line) that it does not listen on udp port 68? We currently have baselined our system to Spectracom SecureSync Version 5.8.5 We would expect that if we don't use DHCP than ntp server is not listening on udp port 68*

- Refer to JIRA SSS-1130

#### Note from Ryan Johnson

Hi @Keith Wing - so we looked in to this further and this is actually how the DHCP system client (dhclient) is intended to operate in our system.

When DHCP is disabled, dhclient is *still running*, and serves the statically configured IP address to the rest of the system. It's important to note though that in this state (DHCP disabled; dhclient serving the static IP internally) even though port 68 remains open (and only tied to dhclient), dhclient is configured to reject any and all incoming packets. When being used with static IPs, dhclient uses this setting in it's configuration:

```
# REJECT EVERYTHING
reject 0.0.0.0/1, 128.0.0.0/1;
```

That effectively blocks any packet from any IP address. Given this is the intended behavior we are going to close the Jira ticket as "Won't Do". I hope this explanation helps with the customer!

### Config files associated wth dhclient

1. /etc/dhclent-eth0.conf
2. /etc/dhclent-eth1.conf
3. /etc/dhclent-eth2.conf
4. /etc/dhclent-eth3.conf

**Examples:**

**A) with Eth0 DHCP disabled (static address)**

**with Eth0 DHCP enabled**

**Note** “Interface” is “eth0” \*(or “eth1” “eth2” “eth3”) matter which interface) and “reject” is set to “0.0.0.0/32”

**Note** “interface” is “ethnone” (no

```
# /etc/dhclient-eth0.conf

interface "eth0" {
    timeout 5;
    retry 10;
    require subnet-mask;
    reject 0.0.0.0/1, 128.0.0.0/1;
}

lease {
    interface "eth0";
    fixed-address 10.0.50.210;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 10.0.50.77, 10.0.50.78;
    option domain-name "noeca.net";
    option routers 10.0.50.1;
    renew 0 2030/1/1 12:00:00;
    rebind 0 2030/1/1 12:00:00;
    expire 0 2030/1/1 12:00:00;
}
```

```
# /etc/dhclient-eth1.conf

interface "eth1" {
    timeout 5;
    retry 10;
    require subnet-mask;
    reject 0.0.0.0/32;
}

lease {
    interface "ethnone";
    fixed address 10.10.202.1;
    option subnet-mask 255.255.0.0;
    #option domain-name-servers;
    option domain-name "domain202";
    option routers 10.10.202.254;
    renew 0 2030/1/1 12:00:00;
    rebind 0 2030/1/1 12:00:00;
    expire 0 2030/1/1 12:00:00;
}
```

**Report of Gateway address being reset to all 0s or erratic value**

- version 5.8.3 (Jan 2019) fixed an issue with interfaces (s configured as Static, being assigned DHCP values)

**Per the Version 5.8.3 Release Notes**

“[Repaired intermittent issue with DHCP addresses being obtained despite static settings](#)”

**B) etc/conf.d/net (“net file”)**

- top of this file stores the main default gateway interface port setting
- settings for each ethernet interface



- these two files are intentionally not included in configs bundle, to prevent them from being cloned into another unit.
- if the file is blank, all interfaces are set to static, disabled or there is an issue with DHCP

```
spadmin@CustService226 /var/lib/dhcp $ cat dhclient.leases
lease {
  interface "eth1";
  fixed-address 10.2.100.202;
  option subnet-mask 255.255.0.0;
  option dhcp-lease-time 345600;
  option routers 10.2.1.1;
  option dhcp-message-type 5;
  option dhcp-server-identifier 10.1.1.26;
  option domain-name-servers 10.1.1.26,10.1.1.27;
  option dhcp-renewal-time 172800;
  option dhcp-rebinding-time 302400;
  option ntp-servers 10.10.225.225;
  option domain-name "int.oroelia.com";
  renew 5 2018/12/14 20:16:56;
  rebind 0 2018/12/16 08:55:55;
  expire 0 2018/12/16 20:55:55;
}
lease {
  interface "eth1";
  fixed-address 10.2.100.202;
  option subnet-mask 255.255.0.0;
  option routers 10.2.1.1;
  option dhcp-lease-time 345600;
  option dhcp-message-type 5;
  option domain-name-servers 10.1.1.26,10.1.1.27;
  option dhcp-server-identifier 10.1.1.26;
  option dhcp-renewal-time 172800;
  option ntp-servers 10.10.225.225;
  option dhcp-rebinding-time 302400;
  option domain-name "int.oroelia.com";
  renew 5 2018/12/14 16:46:50;
  rebind 0 2018/12/16 12:29:02;
  expire 1 2018/12/17 00:29:02;
}
lease {
  interface "eth0";
  fixed-address 10.2.100.203;
  option subnet-mask 255.255.0.0;
  option routers 10.2.1.1;
  option dhcp-lease-time 345600;
  option dhcp-message-type 5;
  option domain-name-servers 10.1.1.26,10.1.1.27;
  option dhcp-server-identifier 10.1.1.26;
  option dhcp-renewal-time 172800;
  option ntp-servers 10.10.225.225;
  option dhcp-rebinding-time 302400;
  option domain-name "int.oroelia.com";
  renew 5 2018/12/14 13:17:47;
  rebind 0 2018/12/16 12:29:05;
  expire 1 2018/12/17 00:29:05;
}
spadmin@CustService226 /var/lib/dhcp $ █
```

### Report of Gateway address being reset to all 0s or erratic value

- version 5.8.3 (Jan 2019) fixed an issue with interfaces (s configured as Static, being assigned DHCP values)

### Per the Version 5.8.3 Release Notes

“Repaired intermittent issue with DHCP addresses being obtained despite static settings”

---

## Ethernet Bonding (two IP addresses assigned to same port) / Link Aggregation

- 803.2ad / Load balancing / Ethernet Bonding/ LCAP (Link Aggregation Control Protocol) Aggregate addresses are NOT supported in SecureSync or Model 9400 series. These are all names for a network function that allows more than one network port to have the same IP address for network redundancy.
- Refer to Mantis case 3091 for a request for us to support Ethernet Bonding.
- The IP addresses for Eth0-Eth3 CAN be on the same subnet but CANNOT be set to the same IP address as another one of the ports (two different ports can't both be 10.10.2.1 for instance).
- Refer to NTP over Anycast as an alternate solution:

(11 Aug 15 KW) Per Dave Sohn, Bonding in SecureSync is feasible. It's just lower in priority right now.

### Duplicate IP addresses

If you duplicate an IP address, network connectivity stops as soon as the IP address has taken ("please wait" is shown on the front panel for about 10 seconds while the changes take effect. Once the message clears, no longer able to ping, access the web browser on any of the ports with the same IP address.

**Note (per Dave Sohn)** : if more than one network port is on the same subnet as other network ports, the routing tables and routing rules will allow response packets to go out the same port that the incoming packets were received on (not just the first port on the subnet).

**Example:** If Eth0 and Eth1 are on the same subnet and NTP request is received on Eth1, the packet will also go back out on Eth1 (not Eth0, even though it's the first port in the routing table). This is established by the routing rules, which "flag" which specific routing table to use for the return, when the packet is initially received.

## C) Ethernet Bonding

(email reply Keith sent about bonding in 2400 SecureSyncs Oct 2022) I am not aware of port bonding/LACP being added in 1.6.0, and haven't heard of any specific plans/intentions to add it in a future update. There has been some limited discussions about it, but Port bonding is typically used for layer 1 packets (such as with routers/switches).

The SecureSyncs are a layer 2 application provider (not intended to be a switch/router), with active/backup fault-tolerance being inherently available within the time client software applications syncing to their NTP/PTP time servers (the client software application can be optionally configured to get time from more than one ethernet interface on the SecureSync. If an interface happens to become unavailable for some reason, it then inherently has immediate ability to receive its time stamps from another configured IP address/interface. This completely alleviates the need for port bonding/LACP.

---

## Netmask settings

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

---

## Auto-MDIX

Ethernet ports Eth1, Eth2 and Eth3 (when the Model 1204-06 Gigabit Option Card is installed) are **auto-MDIX** network ports. This allows a PC to be connected directly to these Ethernet ports without the need for a network cross-over cable.

**Note:** eth0 (the base Ethernet port) is not auto-MDIX, a crossover cable needs to be used when connecting a PC directly to this Ethernet port.

---

## Connecting a PC directly to one of the Ethernet ports

**When connecting a PC directly to ETH0, a network cross-over cable is required:**

- 1) When connecting a PC directly to ETH1, ETH2 or ETH3, since these ports are auto-MDIX, either a straight-thru OR standard network cable can be used.
- 2) Most PCs default to DHCP enabled. The PC needs to be configured with IP address with the same subnet mask as the NTP Server.
- 3) The NTP server's default subnet mask is "16" (255.255.0.0) Not 255.255.255.0. Since 255.255.255.0 is fairly common, a PC directly connected to the network ports may need to be reconfigured as 255.255.0.0 to allow a connection.

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

Table 2-3: Subnet mask table

---

### Status LEDs for the network ports (Eth0- Eth3)

- Note the status LEDs next to Eth0 are dim by design.
- Eth1-Eth3 do not have status LEDs next to Ethernet jacks due to space limitations on Option Cards. But each port has an internal status LED that can be viewed through the slot next to each connector or through holes in the back of the top cover.

Q. I noticed ALL the SecureSync GPS receivers LAN port LED's do not light when connected. I was troubleshooting some connectivity issues here and when I saw no LED's on the receiver I couldn't ping, I thought it was a physical issue until about a half hour later realized None of the SecureSync LAN ports light even when all is OK.

**A (Keith's reply 11/6/12)** For your information, the base Ethernet network port (which is installed in the left-side of the chassis of all SecureSyncs and is called "Eth0") does have an external green Good Link LED and an amber activity LED. These LEDs are always enabled on all SecureSyncs, with no ability to disable them.

However, due to space/footprint limitations on the optional three network port "Gigabit" Option Card (Spectracom Model 1204-06), when installed in a rear panel Option Bay, these three network ports (Eth1, Eth2, and Eth3) do not have external network status LEDs available. But each of these three ports does have its own internal link status LED which is lit when a network cable is connected to the network ports on this Option Card (the link LED being lit can be viewed either right beside each network connector or through the holes in the back of the top cover. These LEDs are always enabled on all SecureSyncs, with no ability to disable them.

This is why you are not seeing any enable/disable boxes associated with the network LEDs in the web browser.



---

## **\*\*Troubleshooting issues with network configuration/operation**

### **A) Desire to know if a network interface (eth0, eth1, eth2 or eth3) is up or down**

- Refer to “Desire to know if a network port is up or down” in the SecureSync Option Card document [..\SecureSync Option Card information.pdf](#)

### **B) Network settings aren't being restored correctly after reboot (going back to default??)**

A customer reported that after each reboot, Eth0 was losing its IP address and all three Gb Option card ports (eth1, eth and eth3) were disabled again (all are enabled before the reboot).

**Conclusion/resolution:** Dave Sohn indicated the factory default settings are eth 0 set to DHCP enabled and all of the Gb ports being disabled. So it appeared they are going to defaults at start-up. Dave S recommended performing a software update to the latest version while also performing a restore to factory default settings. Suspected something may have happened to the configs.

**Note:** Don't restore from a backup file or it the issue could happen again. Manually reconfigure as desired.

### **C) Can't enable certain subnet masks**

#### **1. (Versions 5.x)**

##### **A. Does not accept “/31” (255.255.255.254)**

- At least versions 5.9.3 and below.
- /31 is a “unique” configuration which only works with a “point-to-point” connection (as there are only two IP addresses allowed with this mask). Can't even have a switch in between (just a dumb HUB).
- Refer to Salesforce Case 272436
- Refer to JIRA ticket

##### **B. Does not accept “/30” (versions 5.8.8 and below)**

- Refer to Salesforce Case 191563
- Refer to JIRA ticket SSS-630

**email from Morgan (except from case 191563)** Sadie's demo customer found a software bug when trying to use a /31 subnet address, the /30 would work on his device. When I tied this on our device, /30 nor /31 would work, they would not work from the CLI as well.

- Fixed in v5.8.9 update (June 2020)

#### **2. (Versions 4.x)**

Can't enable certain subnet masks (such as 255.255.255.192) via the front panel interface (configuring via the web browser is fine). Mark Goodlein is aware this is an issue in version 4.0.0, but not sure if he will have time to add to 4.1.0. This will likely get fixed in version 4.2.0 release instead. Reported by Sam Simione from Contech.

---

## IPTABLES (desire to filter packets from getting into the SecureSync/9400s)

- Ability to edit IPtables was added in update version 5.4.0
- Configuration is only available via the CLI (not available via the web browser)
- Can only make security stronger than factory default (can't make security less restrictive than factory default)

**From Wikipedia:** `iptables` is a [user-space](#) application program that allows a [system administrator](#) to configure the tables provided by the [Linux kernel firewall](#) (implemented as different [Netfilter](#) modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; `iptables` applies to IPv4, `ip6tables` to IPv6, `arptables` to [ARP](#), and `ebtables` to [Ethernet frames](#).

### Permissions to edit IPTables

**Note:** Customers can't type "`sudo su iptables`" (which will prompt for login to root).

### Need to type "sudo" before each command

#### A) Versions 5.4.5 and above:

- Starting in v5.4.5, spadmin account now has rights to run iptables. No longer need to type "sudo" in front of "iptables" commands to edit the tables (now just type `iptables xxxx`)

#### B) Versions 5.4.1 and below:

- As of at least v5.4.0, only spadmin account (not custom user accounts) has permission to edit.

#### Prior to version 5.4.0 update: IPTables couldn't be edited as spadmin

- Email Keith sent to Dave Sohn: "This SecureSync customer wants to access the SecureSync's IPTables to block access to malicious IPs".

**A. reply from Dave Soihn (6 Jan 2016)** "Access to IPTABLES is not available to a customer in the SecureSync. The access control feature blocks access to the unit services, but doesn't filter the packets."

---

### Saving changes to the IPTables

- In at least versions 5.8.6 and below, the IPtables are not saved/do not persist through a reboot/power cycle. The changes need to be re-configured after each boot-up.
  - This MAY to be addressed in a future release – as of 20 March 17, it has not yet been determined when the saving of changes will be implemented. Refer to JIRA cases **SSS-523** and **SSS-238** for details

### Customers can create a custom Cron Job/Start-up script (the BEST method to address changes to IPTables, is to make the changes after each boot-up, as part of the startup of the system)

- Per Pritam and Ron Dries (Oct 2019) this approach below is actually better than using the IP Tables Save command (which is not available to customers in at least versions 5.8.6 and below)

**email from Pritam to Morgan (10 Sept 2018)** There is workaround for users to save the iptable rules permanently and have it run when the system reboots:

1. Customer can create a shell script that contains the desire iptables rules.
2. Save this scripts as file in the home directory and give the user executable permission to the file.
3. Run this script via cron, whenever the system gets rebooted, with crontab entry of something like below:  
`@reboot /home/spectracom/firewall.bash`

Let me know if I can assist you with the how-to process in person.

Hi Rich,

You should be able to permanently save the iptables rules with the steps below:

- 1) Create a shell script that contains the desired iptables rules.
- 2) Save this script as a file in the home directory and give the user executable permission to the file.  
(/home/spectracom)
- 3) Run this script via cron, whenever the system gets rebooted, with crontab entry of something like below:  

```
@reboot /home/spectracom/firewall.bash
```

**Reply from a customer (3 Dec 2020)** And to refresh my knowledge, "cron" is a type of Linux scheduler utility that executes on boot, right? So this is pretty much just a quick & dirty fix that doesn't truly save this rule to the iptables, it's just scripted to automatically write the rule to the table immediately on boot-up every single time, thus automating the process? I mean if it gets the job done then it gets the job done, I just want to make sure I'm understanding the logic correctly and that it's not something that can be removed on accident without anyone noticing.

### Operation of editing IPtables

- Consists of editing tables containing of chains of rules for the treatment of packets
- Each table is associated with a different kind of packet processing.
- Packets are processed by sequentially traversing the rules in chains. A rule in a chain can cause a goto or jump to another chain, and this can be repeated to whatever level of nesting is desired. (A jump is like a "call", i.e. the point that was jumped from is remembered.) Every network packet arriving at or leaving from the computer traverses at least one chain.
- Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

### The five individual tables are as follows:

**filter:** This is the default table (if no -t option is passed). It contains the built-in chains INPUT (for packets destined to local sockets), FORWARD (for packets being routed through the box), and OUTPUT (for locally-generated packets).

**nat:** This table is consulted when a packet that creates a new connection is encountered. It consists of three built-ins:

**PREROUTING** (for altering packets as soon as they come in)

**OUTPUT** (for altering locally-generated packets before routing), and

**POSTROUTING** (for altering packets as they are about to go out).

**mangle:** This table is used for specialized packet alteration. Until kernel 2.4.17 it had two built-in chains: PREROUTING (for altering incoming packets before routing) and OUTPUT (for altering locally-generated packets before routing). Since kernel 2.4.18, three other built-in chains are also supported: INPUT (for packets coming into the box itself), FORWARD (for altering packets being routed through the box), and POSTROUTING (for altering packets as they are about to go out).

**raw:** This table is used mainly for configuring exemptions from connection tracking in combination with the NOTRACK target. It registers at the netfilter hooks with higher priority and is thus called before ip\_conntrack, or any other IP tables. It provides the following built-in chains: PREROUTING (for packets arriving via any network interface) OUTPUT (for packets generated by local processes)

**security:** This table is used for Mandatory Access Control (MAC) networking rules, such as those enabled by the SECMARK and CONNSECMARK targets. Mandatory Access Control is implemented by Linux Security Modules such as SELinux. The security table is called after the filter table, allowing any Discretionary Access Control (DAC) rules in the filter table to take effect before MAC rules. This table provides the following built-in chains: INPUT (for packets coming into the box itself), OUTPUT (for altering locally-generated packets before routing), and FORWARD (for altering packets being routed through the box).

## TARGETS

A firewall rule specifies criteria for a packet and a target. If the packet does not match, the next rule in the chain is the examined; if it does match, then the next rule is specified by the value of the target, which can be the name of a user-defined chain or one of the special values ACCEPT, DROP, QUEUE or RETURN.

**ACCEPT** means to let the packet through.

**DROP** means to drop the packet on the floor.

**QUEUE** means to pass the packet to userspace. (How the packet can be received by a userspace process differs by the particular queue handler. 2.4.x and 2.6.x kernels up to 2.6.13 include the ip\_queue queue handler. Kernels 2.6.14 and later additionally include the nfnetlink\_queue queue handler. Packets with a target of QUEUE will be sent to queue number '0' in this case. Please also see the NFQUEUE target as described later in this man page.)

**RETURN** means stop traversing this chain and resume at the next rule in the previous (calling) chain. If the end of a built-in chain is reached or a rule in a built-in chain with target RETURN is matched, the target specified by the chain policy determines the fate of the packet.

---

## Configuration of iptables

**Note: Can lock yourself out if not careful. If this happens, can either:**

- (in at least versions 5.8.6 and below), since the changes to IPtables don't persist through reboots, just reboot the unit to restore the original configurations and regain access.
- Perform a standard **Clean** or **use the front panel Serial port** to edit the tables back to the default configuration (IPtables don't affect the serial port connection).

This function uses the standard linux commands to edit the table. Refer to sites such as:

<http://ipset.netfilter.org/iptables.man.html> or  
[https://fedoraproject.org/wiki/How\\_to\\_edit\\_iptables\\_rules](https://fedoraproject.org/wiki/How_to_edit_iptables_rules)

IPtables is located in the **/sbin** directory (cd to this directory)

**iptables -h** returns iptables help menu

(versions 5.4.1 and below, need to type **Sudo** at the beginning of each command)

### A) Software versions 5.4.5 and above:

- No longer need to type *sudo* in each command (spadmin was give the right to edit iptables starting in update version 5.4.5).
- For example, to list all the current Rules, type: **iptables -L** (or **iptables -list**)

### B) Software versions 5.4.1 and below:

- have to type **sudo** before each command to have root privilege

To list all the current Rules, type: **sudo iptables -L** (or **sudo iptables -list**)

```
spadmin@CustService176 /sbin $ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
spadmin@CustService176 /sbin $
```

Format for Adding a rule (Note: info below shows “sudo” in front of all commands. This word only needs to be typed in versions 5.4.1 and below. Omit this word in versions 5.4.5 and above)

**sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT**

(Append to Input chain a rule that **accepts** TCP port 80 packets)

Where:

-A is to **Append** a new rule to the chain

INPUT is the chain to be edited

-dport defines the port

-j indicates the target (can be: ACCEPT DROP QUEUE or RETURN)

Now display the new rules: **sudo iptables -L**

**Blocking an incoming or outgoing port (such as port 80 for HTTP, or 123 for NTP) on a particular interface (such as just eth0)**

➤ Refer to: <http://www.cyberciti.biz/faq/iptables-block-port/> (also below)

## A) Block incoming packets

To block port 80 (HTTP server), enter (or add to your iptables shell script):

```
# /sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
# /sbin/service iptables save
```

### Block Incoming Port 80 except for IP Address 1.2.3.4

```
# /sbin/iptables -A INPUT -p tcp -i eth1 -s ! 1.2.3.4 --dport 80 -j DROP
```

## B) Block outgoing packets

## Block Outgoing Port

The syntax is as follows:

```
/sbin/iptables -A OUTPUT -p tcp --dport {PORT-NUMBER-HERE} -j DROP

### interface section use eth1 ###
/sbin/iptables -A OUTPUT -i eth1 -p tcp --dport {PORT-NUMBER-HERE} -j DROP

### only drop port for given IP or Subnet ##
/sbin/iptables -A OUTPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s
/sbin/iptables -A OUTPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s
```

To block outgoing port # 25, enter:

```
# /sbin/iptables -A OUTPUT -p tcp --dport 25 -j DROP
# /sbin/service iptables save
```

You can block port # 1234 for IP address 192.168.1.2 only:

```
# /sbin/iptables -A OUTPUT -p tcp -d 192.168.1.2 --dport 1234 -j
DROP
# /sbin/service iptables save
```

## How Do I Log Dropped Port Details?

Use the following syntax:

```
# Logging #
### If you would like to log dropped packets to syslog, first log it ###
/sbin/iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "PORT 80 DROP:

### now drop it ###
/sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
```

## C) Logging dropped port details

### How Do I Log Dropped Port Details?

Use the following syntax:

```
# Logging #
### If you would like to log dropped packets to syslog, first log it ###
/sbin/iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "PORT 80 DROP:

### now drop it ###
/sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
```

---

## **\*\*IPv6 addresses (such as SLAAC address / Link-Local address. Global unicast address)**

- Refer to “IPv6 addresses (for all products that support IPv6)” in custserviceasst doc: <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>
  - Contains info on the four types of IPv6 addresses (Global unicast, Link-local, unique local addresses, and Special addresses)

---

### **IPv6 status**

**(23 Jan 2013):** there are a few Mantis cases open regarding the support of IPv6 addresses. These include:

#### **1722: Issues with IPv6 addresses not being stored and no current support for IPV6 Radius**

**Update to this case (4 Apr 2013) Per Dave Sohn:** The pam\_auth\_radius module we use does not support IPv6. There is an IPv6 patch for it that would need to be tested. So the answer is we do not support IPv6 RADIUS at this time.

**1849/1897: Syslog** not working with IPv6 addresses.

**Status update per Dave Sohn (8 Mar 2013):** “Our current syslog package does not support IPv6. Either a new package/version or patch are required.” (This is recorded in Mantis case 1897)

**1897/1937:** Does the **gateway address** “IPv6 Default Gateway”, support IPv6? Update- Starting in v4.8.9, the main default gateway does support IPv6 addresses. 1937 is now resolved.

**1937 -> 1963: IPv6 static routes**, “desire to configure the IPv6 addresses on the NTP server to ping to another device using different IPv6 subnet

**Update:**

- Mantis 1937 was split off to 1963 to be able to close 1937.
- Mantis 1963 for static routes is still open as of Nov 5. 2014.

### **Summary of IPv6 status as of Archive software version 4.8.9**

**Note (Sept 2014 Update to the info below)** Version 5.1.2 added ipv6 DHCP functionality and SLAAC address

**Email Keith sent to Matt Loomis (16 Apr 2013) and OK'd by Dave Sohn:**

- 1) All **four available network ports** can be assigned IPv4 and/or IPv6 addresses (all of the ports support simultaneous IPv4 and IPv6 addressing).
- 2) With the exception of NTP Autokey, **NTP** supports IPv6.
- 3) The main **default gateway** can be IPv4 or IPv6 (added in v4.8.9 software update). However, **we don't currently support IPv6 static routes** (likely added later this year- Q3 or Q4 expected). Until these are implemented, if the IPv6 network(s) are connected directly to the SecureSync, they are all set. But if they are on subnets not directly connected, we will send unsolicited traffic out on Eth0 instead of to the Ethernet port that routes to the subnet. If they send a packet to the NTP server, we can route back to the correct network port that the packet was received on.
- 4) **Syslog** does not support IPv6. This will require either a patch or a new version of the package that we use for this function. Probably not going to be available for a while.
- 5) Cannot disable IPv6 Auto configuration.

**Additional Note (not included in email to Matt):** We do not support IPv6 Radius at this time.

## \*\*Main Default port/main default Gateway address

This tab of the browser is used to configure network settings for when network traffic originates inside of the SecureSync (instead of responding to traffic that was received. Examples of this include NTP broadcast mode or SNMP traps).

Main Default Gateway address is configured in the:

### A) Classic Interface browser

Network -> General Setup page of the browser, General tab

### B) Newer black/charcoal browser (v5.1.2 and above):

- Management -> Network page of the browser, "General Settings" button (on the left side of the screen):



### C) Configuring the main default gateway via the CLI interface

- CLI command to read which port is the main default gateway: **gw4get m** <enter> (the response is inside the parenthesis)

```
spadmin@Spectracom ~ $ gw4get m
Main default gateway: 10.2.1.1
```

- CLI command to set which port is the main default gateway: **gw4set m x** <enter> (where m is for "main" w and x is the Ethernet interface port number configured with the desired main default gateway address)

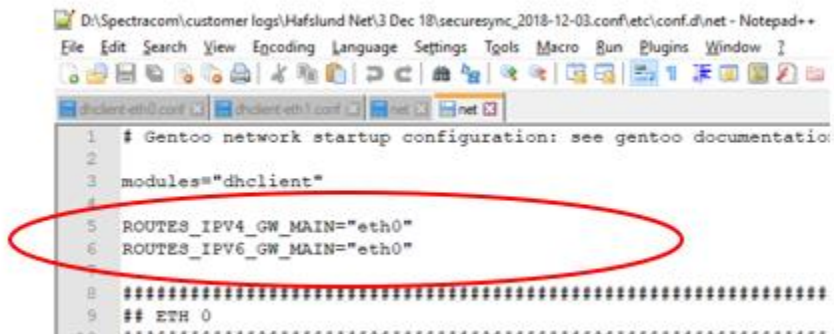
```
spadmin@Spectracom ~ $ gw4set m 0
```

Example to make the default gateway port as port 2: **gw4set m 2** <enter>

- CLI command to set the default gateway for a particular port (not the main default gateway) the command is **gw4set m 2** <enter> (where x specifies the main default gateway port is being configured, and 2 is the interface having the desired gateway address.



Main default port config is stored/located (at the very top of the file. as ROUTES\_IPV4\_GW\_MAIN and "ROUTES\_IPV6\_GW\_MAIN") in: `./etc/conf.d/net`



### Difference between the global gateway address and the interface gateway addresses

(9/27/12 Email from Dave Sohn to Sylvain) The gateway answer is also fairly easy. It is the difference between a global and interface gateway address. The unit will use the interface specific gateway to determine where to send packets outside of its subnet if the packet came in on that interface. The unit will use the global gateway to determine where to send packets outside of its subnet if the packet is being generated independently by the SecureSync.

### Conditions/Troubleshooting main default gateway issues

#### General troubleshooting

- Keep in mind that it can take a bit of time (such as around a minute or so) for a change to network settings to take effect- and not all user interfaces update automatically/right away . Make sure to refresh the web browser, the front panel LCD menu, cli commandd, etc a couple minutes after making a change to confirm settings were accepted.
1. Get logs/configs
  2. Verify network settings using various methods- not just one (such as web browser, **gw4get** CLI command, front panel gateway menu)

#### Specific condtion/troubleshooting

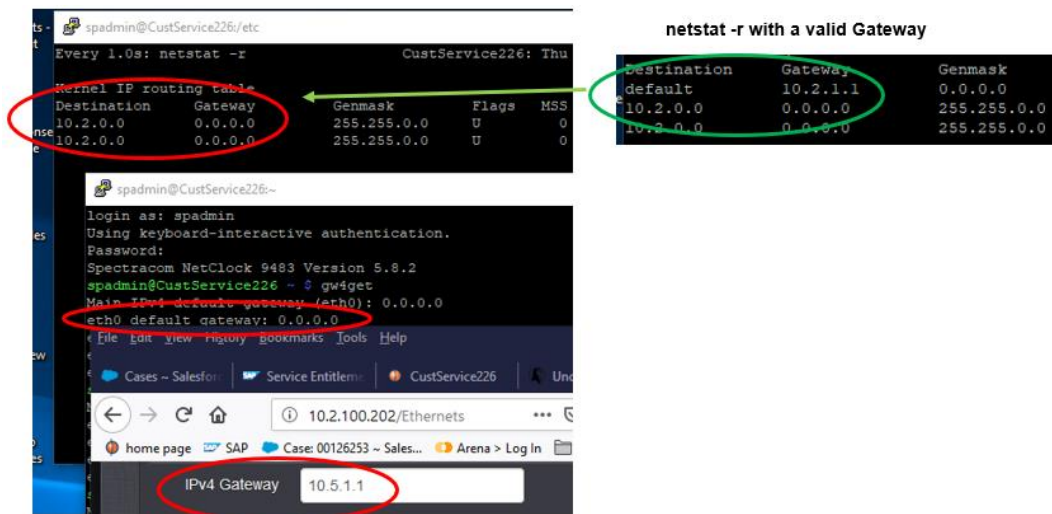
##### A) If an invalid gateway address is entered for the selected interface port (in at least v5.8.2)

- Front panel LCD continues to report the gateway address as all 0's (0.0.0.0)
- Web browser continues to show the invalid value it was set to- even if the page is refreshed a short while later

##### B) Gateway address for the selected default interface not valid/front panel LCD displayingas all 0's (all zeroes, as in "0.0.0.0")

If the configured gateway address is not valid (example below is gateway entered "10.5.1.1" instead of "10.2.1.1")

- **Front panel:** LCD "Gateway" menu **displays all 0's** if its not a valid gateway address
- **gw4get** CLI command: displays all 0's if its not a valid gateway address
- **netstat -r** cli command: displays all 0's if its not a valid gateway address
- **web browser** displays the incorrect/invalid address which was entered



- Make sure configured gateway address for that interface is valid (Keith confirmed 12 Dec 2018 w/v5.8.2 that the gateway doesn't need to be "reachable: over the network to configure it (network cable was unplugged when configuring it) - the gateway address just needs to be a valid address for the subnet the interface is on.

### C) (much earlier versions such as v5.2.1 and below): Issues with setting the main default gateway port via the newer black/charcoal web browser

- Refer to Mantis cases 3086 and 2788
- 3086 is associated with at least v5.2.1 and 2788 associated with 5.1.3 to 5.2.0??
- Changing back to eth0 seems ok. But it doesn't like selecting eth 1, 2 or 3.
- Work-around is to use the cli command of **gw4set m x** <enter> (where m stands for "main" and where x is the desired port to use as gateway)

### D) (v4.8.8 and below) Note about IPv6 Default gateway address field:

- versions 4.8.8 and below have an issue with being able to configure this field. It was addressed in the version 4.8.9 release (March 2013).

### E) Validation error when trying to configure the Default gateway

**Email from Keith to Roots (3 Apr 2013)** Thanks for reporting their observation to us.

In order to configure the IPv6 default main gateway, all of the individual IPv6 network settings need to first be properly configured. When the IPv6 default gateway address is attempted to be configured, the SecureSync performs system checks to ensure the entered gateway address is both valid and reachable, based on the interface settings (as configured in the **Network** -> **Interfaces** page of the browser, the tabs for each of the network ports).

If your customer has not yet configured each of the network ports yet and don't have the SecureSync connected to the network that the gateway is on, please have them retry entering the IPv6 after they have configured the other settings. If it then accepts the gateway address, just let me know they are all set.

However, if they still get a validation error, please have them send us screenshots of all the tabs in the **Network** -> **Interfaces** page of the browser, as well as a screenshot of the **Network** -> **General Setup** page of the browser, General tab. We will review the values they are entering to try to determine why they are seeing a validation error.

## \*\* individual gateway addresses (IPv4/IPv6) for each interface

**Purposes** Used for responding to received network traffic (not used for broadcast traffic)

### Difference between the main default gateway (global gateway) address and the interface gateway addresses

**(9/27/12 Email from Dave Sohn to Sylvain)** The gateway answer is also fairly easy. It is the difference between a global and interface gateway address. The unit will use the interface specific gateway to determine where to send packets outside of its subnet if the packet came in on that interface. The unit will use the global gateway to determine where to send packets outside of its subnet if the packet is being generated independently by the SecureSync.

**DHCP:** Enable/Disable DHCP on each port

**DNS Setup:** Defines DNS servers on this particular port's network

**Domain Setup:** Not the DNS Host name (this is defined elsewhere) example: roc.spectracom.us

**IP Address setup:** Define the IPv4 address or IPv6 addresses for each port.

**“Static Routes” table in each tab:** Used to define networks on other side of routers that are attached to any or all of the Ethernet ports (but are not available through the default gateway). “Network address” will likely end in 0's (don't include the “/” and bits to define the subnet mask. These are entered with just the number in the “Prefix field”. Enter the router's IP address in the “Router Address” field.

In the example screenshot below, Eth 0 has a router at 10.2.100.1 that is also attached to a 192.168.1.x network. And, it's desired for responses to network traffic to be sent to this other subnet.

| Interface | IP Version | Network Address | Prefix | Router Address | Delete                   |
|-----------|------------|-----------------|--------|----------------|--------------------------|
| eth0      | IPv4       | 192.168.1.0     | 24     | 10.2.100.1     | <input type="checkbox"/> |
| eth0      | IPv4       |                 | 0      |                | <input type="checkbox"/> |
| eth0      | IPv4       |                 | 0      |                | <input type="checkbox"/> |
| eth0      | IPv4       |                 | 0      |                | <input type="checkbox"/> |
| eth0      | IPv4       |                 | 0      |                | <input type="checkbox"/> |

## A) Configuring IPv4 gateway addresses

### 1. Via front panel keypad/LCD

➤ **Refer to online user guide:**

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm?Highlight=gateway](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm?Highlight=gateway)

### 2. Via CLI interface (telnet/ssh/serial)

#### **gw4set** command

The command to configure IPv4 interface gateway address is: **gw4set y xxx.xxx.xxx.xxx** (where is the interface number) **Example for eth0: gw4set 0 10.2.1.1**

**gw4get** command: lists all the interface gateway addresses

### 3. Via the web browser

**Newer (black/charcoal) web browser:**

**Management** -> **Network Setup** page

Each of the tabs (eth 0 always- eth1, eth2, and eth3 when Gigabit card installed) on this page of the browser are used to configure network settings of each network port for when SecureSync is responding to network traffic that it receives (Examples of this include NTP unicast mode or web browser).

**Important note: it can take a couple minutes for the Gateway to change. Then gateway value in the browser will continue to report the previous value. Need to refresh the page a little later for the browser to show the new**

value

## Verifying/viewing an interface gateway address

### 1. Via front panel keypad/LCD

- Refer to online user guide:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm?Highlight=gateway](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/FrontPanelIPconfig.htm?Highlight=gateway)

### 2. Via CLI interface (telnet/ssh/serial)

**gw4get** command: lists all the interface gateway addresses

**netstat -r** command (**kernel routing table**): Apparently, this command lists just the **main default gateway** address (so it only reports the interface gateway of the selected default interface port (such as "eth0"))

```
kernel IP routing table
Destination      Gateway          Genmask          Flags   MSS Window  irtt Iface
default          10.2.1.1         0.0.0.0          UG      0 0        0 eth0
10.2.0.0         0.0.0.0          255.255.0.0      U        0 0        0 eth0
10.2.0.0         0.0.0.0          255.255.0.0      U        0 0        0 eth1
spadmin@CustService226 /etc $
```

### 3. Via the web browser

Newer (black/charcoal) web browser:

*Management* -> *Network Setup* page

Each of the tabs (eth 0 always- eth1, eth2, and eth3 when Gigabit card installed) on this page of the browser are used to configure network settings of each network port for when SecureSync is responding to network traffic that it receives (Examples of this include NTP unicast mode or web browser).

**Important note:** it can take a couple minutes for the Gateway to change. Then gateway value in the browser will continue to report the previous value. need to refresh the page a little later for the browser to show the new value

## Conditions/Troubleshooting interface gateway issues

### General troubleshooting

1. Get logs/configs
2. Verify network settings using various methods- not just one (such as web browser, **gw4get** CLI command, front panel gateway menu)
  - Keep in mind that it can take a bit of time (such as around a minute or so) for a change to network settings to take effect- and not all user interfaces update automatically/right away . Make sure to refresh the web browser, the front panel LCD menu, cli command, etc a couple minutes after making a change to confirm settings were accepted.

### Specific conditions/troubleshooting gateway issues

#### A) (v5.8.2 and below) Report of Gateway address being reset to all 0s or erratic values

- Version 5.8.3 (Jan 2019) fixed an issue with interfaces (configured as Static) being assigned DHCP values

##### Per the Version 5.8.3 Release Notes

“Repaired intermittent issue with DHCP addresses being obtained despite static settings”

#### B) If an invalid gateway address is entered (in at least v5.8.2)

- Front panel LCD continues to report the gateway address as all 0's (0.0.0.0)
- Web browser continues to show the invalid value it was set to- even if the page is refreshed a short while later

#### C) Gateway address not valid/front panel LCD displaying as all 0's (all zeroes, as in “0.0.0.0”)

If the configured gateway address is not valid (example below is gateway entered “10.5.1.1” instead of “10.2.1.1”)

- **Front panel:** LCD “Gateway” menu displays all 0's if its not a valid gateway address
- **gw4get CLI command:** displays all 0's if its not a valid gateway address
- **netstat -r cli** command: displays all 0's if its not a valid gateway address
- **web browser** displays the incorrect/invalid address which was entered

The image shows a composite of three screenshots illustrating gateway configuration problems. The top-left screenshot shows a terminal window with the command `netstat -r` executed, displaying the kernel IP routing table. The table shows entries for destination 10.2.0.0 with gateway 0.0.0.0. A red circle highlights the routing table header, and a green arrow points to the gateway column. The top-right screenshot shows the output of `netstat -r` with a valid gateway (10.2.1.1), with a green circle highlighting the correct gateway address. The bottom screenshot shows a web browser interface where the IPv4 Gateway field contains the invalid address 10.5.1.1, circled in red. The browser's address bar shows the URL 10.2.100.202/Ethernets.

| Destination | Gateway | Genmask     | Flags | MSS |
|-------------|---------|-------------|-------|-----|
| 10.2.0.0    | 0.0.0.0 | 255.255.0.0 | U     | 0   |
| 10.2.0.0    | 0.0.0.0 | 255.255.0.0 | U     | 0   |

| Destination | Gateway  | Genmask     |
|-------------|----------|-------------|
| default     | 10.2.1.1 | 0.0.0.0     |
| 10.2.0.0    | 0.0.0.0  | 255.255.0.0 |
| 10.2.0.0    | 0.0.0.0  | 255.255.0.0 |

- Make sure configured gateway address for that interface is valid (Keith confirmed 12 Dec 2018 w/v5.8.2 that the gateway doesn't need to be “reachable: over the network to configure it (network cable was

unplugged when configuring it) - the gateway address just needs to be a valid address for the subnet the interface is on.

**CLI command: `netstat -r`** (“kernel IP routing table”)

**Note:** for more info on routing tables/kernel IP routing table refer to sites such as: <https://www.cyberciti.biz/faq/what-is-a-routing-table>

Sample output:

```
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0
0.0.0.0 192.168.1.1 0.0.0.0 UG 100 0 0
```

• **Flags** : Possible flags include

- U (route is up)
- H (target is a host)
- G (use gateway)
- R (reinstate route for dynamic routing)
- D (dynamically installed by daemon or redirect)
- M (modified from routing daemon or redirect)
- A (installed by addrconf)
- C (cache entry)
- ! (reject route)

- Response to `netstat -r` only continues to display the gateway address (for more than just a couple minutes) if the configured gateway address is valid (see “A” below)
- if the address is not valid for the subnet. the gateway entry disappears a couple minutes after its changed/set to the invalid value (See “B” below)

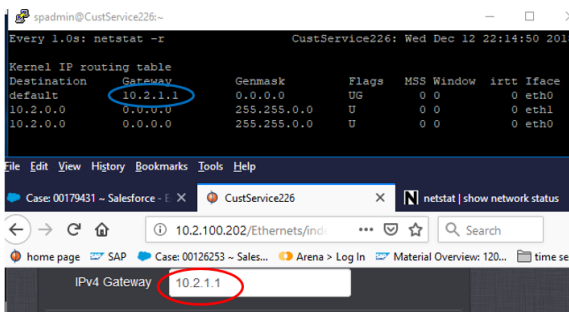
**D) With the correct Gateway address entered (eth0 connected to network)**

- `netstat -r` continues to report the entered gateway address of 10.2.1.1

```
Every 1.0s: netstat -r                               CustService226: Wed Dec 12 20:32:08 2018
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default 10.2.1.1 0.0.0.0 UG 0 0 0 eth0
10.2.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth1
10.2.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
```

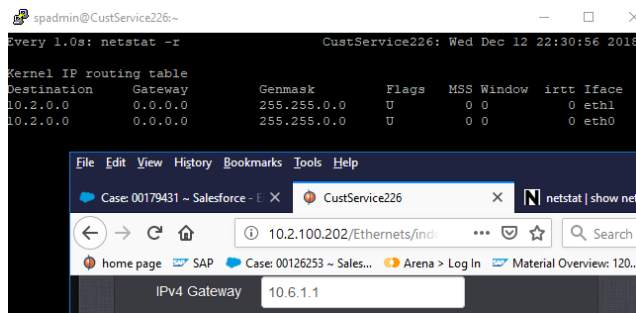
**E) With the correct Gateway address entered via eth1/browser (with eth0 not connected to network) = Works fine**

- `netstat -r` (and web browser) reports (and continues to report) the entered gateway address of 10.2.1.1
- Front panel LCD “gateway” (and IP address) displayed as all 0's just because cable is disconnected



**F) Invalid gateway address (10.6.1.1) configured (not on same subnet as IP address) with eth0 still disconnected**

- “netstat -r” doesn’t report the invalid address
- web browser will continue to report the invalid address entered.



**Desire to “reset” one particular non-DHCP network port (without having to reboot)**

**(10/23/12 KW) Based on feedback from Dave Sohn, reply to a customer**

The SecureSync doesn’t have a command/button to explicitly bring down or up the individual network interfaces (Eth0 through Eth3). Besides performing a system reboot (or power cycle), you may be able to restore the network port operation by simply enabling and then disabling DHCP for the one particular network interface.

DHCP can be toggled in the **Network -> Interfaces** page of the web browser. Then, select the “Eth1” tab for instance. There is an ON/OFF button to turn DHCP on and off.

If toggling DHCP for the port doesn’t restore network connectivity, we would then recommend a reboot of the system (This can be performed in the **Tools -> Reboot/Halt** page of the browser. Press the **Reboot** button to perform the reboot. The system will be back up and running in about two minutes or so (and synced a couple of minutes thereafter).

**Network switch settings for interfacing with SecureSync**

- Q. (from Gregory with BellAlliant) I’m wondering if the Ethernet ports need anything special parameters? The Alcatel is set force the 1 Gbps speed using the Auto negotiate limit function.
- A. (reply from Dave Sohn 22 Jan 2013)** I’m not aware of restrictions or configuration requirements for either the 10/100 or Gigabit ports. The pause frames wouldn’t be a result of misconfiguration, but they could show an issue. I couldn’t find anything definitive in the gigabit driver bug reports about flow control autonegotiation. If they are causing problems maybe we need to disable them, but I’m not sure at this point.

- Q. (from Gregory with BellAlliant) I’ve learned that the Alcatel switch has the ports that are facing the NTP servers set to “auto-negotiate limited”, which restricts some of the features that are to be negotiated.

Do you have a specification document that describes the Gigabit Ethernet (3X) module options that need to be active or disabled when the Layer 2 connection is to be made between the NTP’s interface and another interface (or Alcatel switch in this case)?

Also, can we control the layer 2 options that are active or disabled from the CLI of the NTP?

## G) IPv6 gateway addresses

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

### Gw6set command/Configuring IPv6 gateway address using link-local address

- Command to configure IPv6 gateway address is: **gw6set on/off xxxx:xxxx:xxxx:xxxx:xxx**

```
spadmin@Spectracon ~ $ gw6set
Invalid arguments
Usage: gw6set <on|off> [addr]
addr: IPv6 address, ie. fe80::230:64ff:fe04:3ef8
spadmin@Spectracon ~ $ _
```

### “Failed to enable or disable the IPv6 default gateway” reported

- Issue with setting IPv6 gateway address using the 'link-local' IPv6 address (works when using the Global address but not when using the link-local address)
- Refer to SF case 115892/JIRA SSS-350
- Applicable to versions 5.7.2 and below. Fixed in v5.7.3 (with 5.8.0 being the next subsequent general release)

from the v5.7.3 release notes:

Updated IPv6 networking support to more closely match IPv4 networking. Added additional routing tables per network port with individual IPv6 default gateways. Static IPv6 routes can be applied per network port.

**Email from Dave Sohn (1 Aug 17)** Routing is typically not done within the link-local address space, but we did find a bug in the gw6set function when used with link-local gateway addresses. It will have to be resolved in a future SW update. There is no workaround for utilizing the link-local address at this time. The only workaround is to setup IPv6 static addresses on the SecureSync and the gateway device and use that for the gateway setting.

### From the original report email thread from Nori w/TOYO (1 Aug 17)

(The assigned link-local address is shown on the left-side off the below screenshot. The customer entering the gw6set command with the link-local address is shown on the right-side).

```
interface GigabitEthernet0/1/6
no ip address
keepalive 60
no cdp enable
spanning-tree portfast
!
interface GigabitEthernet0/1/7
no ip address
keepalive 60
no cdp enable
spanning-tree portfast
!
interface Ulan1
ip address 192.168.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
ipv6 address FE80::1 link-local
ipv6 address FD00:0:20:1::1/64
ipv6 enable
!
interface Bsync1
no ip address
encapsulation sllip
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface GigabitEthernet0/1/6
ip nat inside source static tcp 192.168.0.212 5900
5900
ip route 192.168.1.0 255.255.255.0 192.168.0.5
ip route 192.168.2.0 255.255.255.0 192.168.0.5
ip route 192.168.3.0 255.255.255.0 192.168.0.5
ip route 192.168.4.0 255.255.255.0 192.168.0.5
ip route 192.168.5.0 255.255.255.0 192.168.0.108
ip route 192.168.7.0 255.255.255.0 192.168.0.108

spadmin@Spectracon ~ $ gw6set
ip6del 0 fe80::32 120
ip6add 0 fe80::32 10
net6
Spectracon
Main IPv6 default gateway: None
eth0
INET6 fe80::32/10
DHCPCv6(eth0)=Disabled
spadmin@Spectracon ~ $ ping6 -l eth0 fe80::1
PING fe80::1(fe80::1) from fe80::32 eth0: 56 data bytes
64 bytes from fe80::1: icmp_seq=1 ttl=64 time=0|501 ms
^C
--- fe80::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 0.501/0.501/0.501/0.000 ms
spadmin@Spectracon ~ $ gw6set on fe80::1
RINETLINK answers: Invalid argument
Failed to enable or disable the IPv6 default gateway (on, fe80::1)spadmin@Spectracon ~ $ routes6
Main routing table:
fe80::/10 dev eth0 proto kernel metric 256
```

Yes, the customer certainly had connected the SecureSync demo unit to their IPv6 gateway. (FE80::1) Actually, the customer and we could properly apply IPv6 global addresses as gateway, of course we had



established physical connection between the unit and the gateway before starting the setup.

We still have an issue that we cannot use link-local addresses for the gateway settings. Perhaps is there a limitation to use link-local addresses for IPv6 gateway in the SecureSync?

Or, as one of workaround, can we add manually new gateway settings using general linux commands as superuser?

[Current route table of our SecureSync demo unit, two global addresses have been applied as gateway]

```
spadin@Spectracom /etc # cat /etc/centos-release
Centos Base System release 2.2
spadin@Spectracom /etc # route -A inet6
Kernel IPv6 routing table
Destination          Next Hop             Flag Met Ref Use If
fe00::0:20:1::/64   [::]                U    256 0   1 eth0
fe80::/10           [::]                U    256 0   0 eth0
[::]/0              fe00::0:20:1::1    UG   5   0   0 eth0
[::]/0              fe00::0:20:1::1    UG  1024 0   0 eth0
[::]/0              [::]                !n   -1  1   98 lo
localhost/128       [::]                !h   0   11639207 lo
fe00::0:20:1::32/128 [::]                !h   0   1   0 lo
fe80::32/128        [::]                !h   0   1   3 lo
ff00::/8            [::]                U    256 0   0 eth0
[::]/0              [::]                !n   -1  1   98 lo
spadin@Spectracom /etc #
```

**Email from Dave Sohn (1 Aug 17) (referring to software version 5.7.0)** Routing is typically not done within the link-local address space, but we did find a bug in the gw6set function when used with link-local gateway addresses. It will have to be resolved in a future SW update. There is no workaround for utilizing the link-local address at this time. The only workaround is to setup IPv6 static addresses on the SecureSync and the gateway device and use that for the gateway setting.

#### IPv6 Gateway will not save (observed in v5.4.1 and subsequent versions)

- Observed/reported in Jun, 2016 with version 5.4.1 installed
- Refer to Mantis case 3276 and SR 5309 in SAP
- Issue with browser only. Works fine with the CLI interface.

**Email from Dave Sohn (8 Jun 16)** As I stated in our call, the summary is that the IPv6 default gateway configuration using the web UI is not working on SecureSync. The command line interface IPv6 default gateway configuration does work. There are two locations in the web UI to set a default IPv6 gateway and they both have issues. The IPv6 main default gateway setting under the “General Settings” in the network configuration page does not correctly set the gateway in the live configuration or the configuration file. The IPv6 default gateway setting under the per port configuration page, does a set to a routing table setup per port, but those routing tables are not used by the system, and It also does not set the configuration file correctly. However, due to how the gateway is read on the cli, when the per port default gateway is set in the incorrect table, it is read by the command line interface get (gw6get), adding to the confusion. For units that you may have already gotten into this state, this can be cleared by clearing the per port IPv6 gateway field and submitting. You should see the command line interface get (gw6get) return “None” again. Once it returns “None”, you can correctly utilize the command line gateway set (gw6set) command to correctly set the IPv6 main default gateway for the unit. Let us know how this goes tomorrow night, once you can make the attempt during the maintenance window, and we are sorry for the confusion and issues this created.

**Email Dave Lorah sent to the customer** We have confirmed a problem in the web browser settings of the IPv6 parameters. A workaround for setting up an IPv6 Gateway in the Securesync.

The summary is that the IPv6 default gateway configuration using the web UI is not working on SecureSync. However, the command line interface IPv6 default gateway configuration does work.

There are two locations in the web UI to set a default IPv6 gateway and they both have issues. The IPv6 main default gateway setting under the “General Settings” in the network configuration page does not correctly set the gateway in the live configuration or the configuration file. The IPv6 default gateway setting under the per port configuration page, does a set to a routing table setup per port, but those routing tables are not used by the system, and It also does not set the configuration file correctly. However, due to how the gateway is read on the cli, when the per port default gateway is set in the incorrect table, it is read by the command line interface get (gw6get), adding to the confusion. For units that you may have already gotten into this state, this can be cleared by clearing the per port IPv6 gateway field and submitting.

For each Ethernet port, make sure the IPv6 Gateway Field is blank and SUBMIT



After clearing the settings in the web UI you should see the command line interface get (gw6get) return "None" again. Once it returns "None", you can correctly utilize the command line gateway set (gw6set) command to correctly set the IPv6 main default gateway for the unit.

---

## RFC-2462 (RFC 2462): IPv6 SLAAC Addresses (Stateless Address Autoconfiguration for IPv6)

- Refer to: <https://datatracker.ietf.org/doc/rfc2462/> and “RFC-2462: SLAAC Addresses” in <..\CustomerServiceAssistance.pdf>
- Refer to: [http://en.wikipedia.org/wiki/IPv6\\_address#Stateless\\_address\\_autoconfiguration](http://en.wikipedia.org/wiki/IPv6_address#Stateless_address_autoconfiguration)
- Refer also to Salesforce Cases such as 192442 (Apr 2019)

On system startup, a node automatically creates a [link-local address](#) on each IPv6-enabled interface, even if globally routable addresses are manually configured or obtained through "configuration protocols" (see below). It does so independently and without any prior configuration by stateless address autoconfiguration (SLAAC),<sup>[29]</sup> using a component of the [Neighbor Discovery Protocol](#). This address is selected with the prefix  $\text{fe80}::/64$ .

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

---

### SecureSync compliancy with RFC 2462

- Refer to Salesforce Cases 192442

Regarding the other two SecureSync questions you sent to me (pertaining to RFC 2462 and SAASM receiver keys), I assigned our case number **192442** to track both questions and forwarded them to our Apps Engineering team. Will definitely get back to you with more details, once I hear back from them!

As for the question about RFC 2462, I can give you a quick “preview” answer that there SecureSync does support SLAAC IPV6 addresses. We just need to verify the RFC to see what other requirements, if any, it may contain to state full compliance with this RFC.

The SecureSync user guide doesn't specifically mention/discuss “RFC 2462” in itself, but it does mention configuration of IPv6 SLAAC addresses. Here are two links to the online SecureSync user guide which shows this config (the first link is the associated CLI commands and the second is for the associated web browser functionality):

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=slaac](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=slaac)

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/NCSS\\_Netw\\_Ports.htm?Highlight=slaac](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_Netw_Ports.htm?Highlight=slaac)

Reply from Ron Dries (22 April 2019)

Hi Keith,

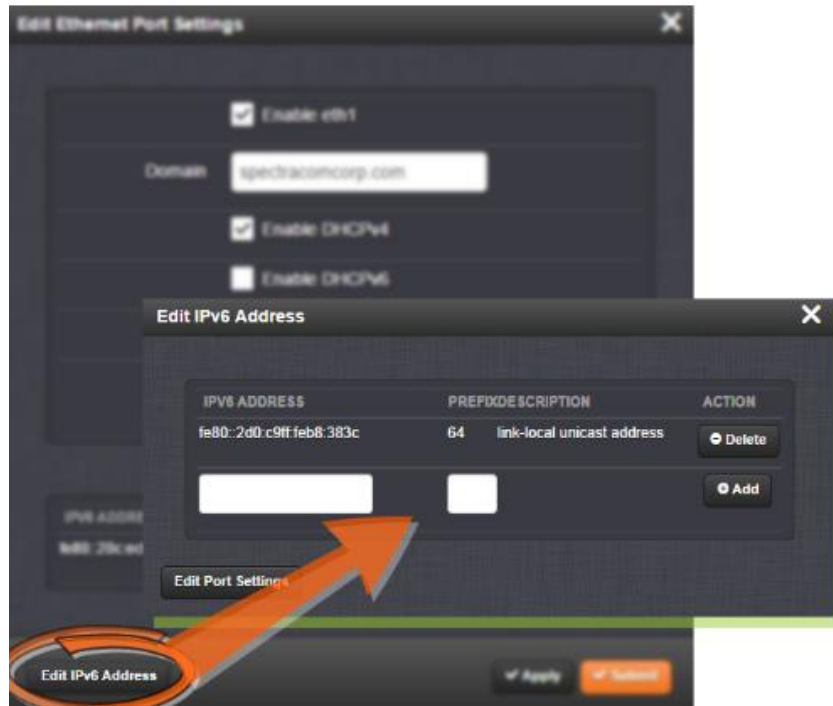
We do not do anything special with SLAAC, it is handled by the Linux kernel and it is difficult to tell if the kernel is fully compliant with RFC 2462. Lets see how she responds to what you told her last week.

---

### Configuring SLAAC address:

The SecureSync user guide doesn't specifically mention/discuss “RFC 2462” in itself, but it does mention configuration of IPv6 SLAAC addresses. Here are two links to the online SecureSync user guide which shows this config (the first link is the associated CLI commands and the second is for the associated web browser functionality):

- [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=slaac](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=slaac)
- [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/NCSS\\_Netw\\_Ports.htm?Highlight=slaac](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_Netw_Ports.htm?Highlight=slaac)




---

## Software changes associated with SLAAC addresses

### A) Version 5.7.3

- Corrected bug in enabling/disabling IPv6 SLAAC

### B) Version 5.1.2

- Added support for IPv6 DHCP functionality and SLAAC addresses.

---

## FAQs about SLAAC

Q. Can you check with the team and ask them for a short description on what they had to change/add to the code to allow for SLAAC to be disabled.

A. **(per Dave Sohn 29 Aug 2014)** We added code to modify our Linux kernel parameters per interface, to ignore IPv6 router advertisements, which generate the SLAAC addresses when received.

---

Q So, the systems are responding after using the "gw6set" commands. But the underlying issues of the following are still a problem, per se:

- 1) missing CONFIG\_ROUTES\_IPV6\_MAIN value. This remains blank no matter how it is set (GUI or CLI)
- 2) SLAAC picks up incorrect gateway, uses link-local IPv6 address
- 3) "General Settings" dialog to set the IPv6 gateway always comes up blank, and doesn't seem to set that value in /etc/conf.d/net. This can be confusing.

It seems the GUI is not a reliable way to set the IPv6 gateway.

**A reply from Dave L (16 Jun 17)** The way it was explained to me is the IPv6 routing functions are not enabled in the Securesync but there is capability to enter the Gateway address. The IPv4 routing is functional but the same routing functions for IPv6 are not. So you cannot use the same "routes" commands as IPv4.

The gw6set and gw6get are the only parameters that can be used. We are working on cleaning this up for the next firmware release. I expect it will be ready in 2 to 3 weeks.

These commands are not valid:

Rt6add  
Rt6get  
Rt6del  
Routes6

Also, do not enter a gateway address in the web browser IPv6 gateway field. This will also cause a problem.

**A reply from Dave L (16 Jun 17)** Your first question was answered in my previous email. Yes, the GUI is not functional for configuring the IPv6 gateway.

The SLAAC function can be explained by this: The SecureSync automatically generates a link-local address that is based on the hardware MAC address. In general, machines using IPv6 will typically have several addresses, one of which is usually a link-local address. The SecureSync does not currently have support for permanently turning off the link-local address. It can be deleted, but will be recreated whenever the interface link is brought up or the system is rebooted. You may use your static IP address but the auto configured link-local address will be there as well.

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

## Static Routes/ Default Routes /Static Routing/ Routing tables

**From Wikipedia:** **Static routing** is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing protocol to forward traffic. In many cases, static routes are usually manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured.

Info below from: [http://www.cs.virginia.edu/~itlab/book/pdf/Ch3\\_v3.pdf](http://www.cs.virginia.edu/~itlab/book/pdf/Ch3_v3.pdf)

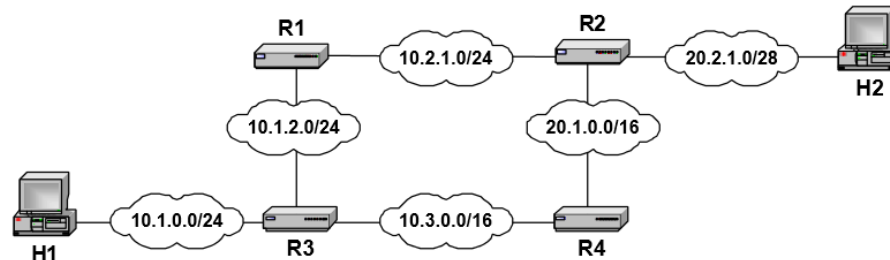


Figure 3.2. Collection of networks (View at the IP layer).

Routing tables, which are kept at both hosts and routers, play a crucial role in the delivery of IP datagrams. A routing table tells a host or router what to do with a datagram that must be transmitted. There is one routing table lookup for each IP datagram. For a given destination IP address, the routing table lookup may yield that the destination IP address is on the same IP network as an interface of the local host or router. In this case the datagram is said to be *directly deliverable*. Alternatively, the routing table lookup may yield the IP address of a *next hop router*, which is a router to which IP datagrams can be directly delivered. In Figure 3.2, host A and router R1 can directly deliver IP datagrams to each other. For host H1, the only next hop router is router R3. Router R1 has two possible next hop routers, routers R2 and R3.

When a routing table yields that a datagram cannot be directly delivered, the IP datagram is encapsulated in a data link layer frame and sent to the next hop router. When the datagram is received, the receiving router also performs a routing table lookup and, forwards the datagram to its own next hop router. In this fashion, the datagram is forwarded hop-by-hop until it reaches a router where the datagram can be directly delivered to the destination. In this hop-by-hop forwarding scheme, each a host or router makes a local decision, and no entity has complete information about the complete path of a datagram.

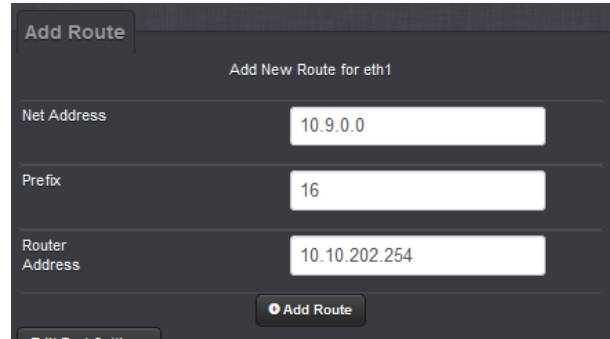
- Static routes are used to route unrequested broadcast type packets (such as SNMP Traps for example) to the appropriate network, if no Static Routes are defined.
- Not required for responding to packets that originate from outside SecureSync (such as NTP packets)
- They are used to route unrequested packets (such as SNMP Traps for example) to the applicable network port on the SecureSync (if not being sent to the Default gateway address).
- Not required for packets that originate from outside SecureSync (such as NTP packets)
- If there are no Static Routes defined, unrequested packets (such as SNMP traps) will be routed to the Default Gateway address (defined towards the top of the same page of the browser)

### Notes about static routes

The SecureSync's static routes are just to get packets to the correct Ethernet interface's gateway address, if it can't be handled by the default gateway/port (doesn't care about routing of the packet after the default gateway since this is handled by the routing tables in the routers themselves).

### Example for a static route to be used:

1. **Eth0** is the configured default port/gateway address (its gateway is 10.2.1.1)
2. But an internally generated packet (not responding to an incoming packet) needs to go out **eth1** instead of **eth0** (example- the address it needs to go to is **10.9.3.4 /16**, via eth1's gateway address of **10.10.202.254**)
3. Normally, the packets would go out eth0 (the default gateway). So a static route needs to be configured in eth1 that tells it to route this address/subnet (such as **10.9.0.0** via eth1's gateway address of **10.10.202.254** with a prefix of **16**



Add Route

Add New Route for eth1

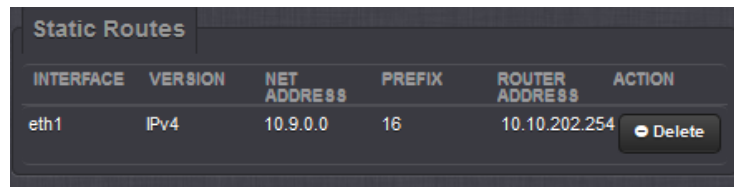
Net Address: 10.9.0.0

Prefix: 16

Router Address: 10.10.202.254

Add Route

After pressing "Add Route"



| INTERFACE | VERSION | NET ADDRESS | PREFIX | ROUTER ADDRESS | ACTION |
|-----------|---------|-------------|--------|----------------|--------|
| eth1      | IPv4    | 10.9.0.0    | 16     | 10.10.202.254  | Delete |

### Notes about static routes

The SecureSync's static routes are just to get packets to the correct Ethernet interface's gateway address, if it can't be handled by the default gateway/port (doesn't care about routing of the packet after the default gateway since this is handled by the routing tables in the routers themselves).

#### Configuring/Viewing default static routes (IPv4 and IPv6)

##### A) IPv4 static routes (for eth0, eth1, eth2 or eth3)

- **Note:** info regarding **IPv6 static routes** is further below in a separate section

#### IPv4 static routes were added in version 4.6.0

- From the update 4.6.0 Release Notes:

"Added Static Route control for all interfaces and a main/common route section"

#### IPv4 Static Routes can be displayed/configured via either the web browser or via CLI commands

- Refer to the SecureSync CLI section of the document for the commands associated with static route, such as **routes4**, **rt4add**, **rt4del** and **rt4get**.

#### IPv6 Static Routes can be displayed/configured via either the web browser or via CLI commands

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

- refer to the SecureSync CLI section of the document for the commands associated with static route, such as **routes3**, **rt5add**, **rt6del** and **rt6get**.

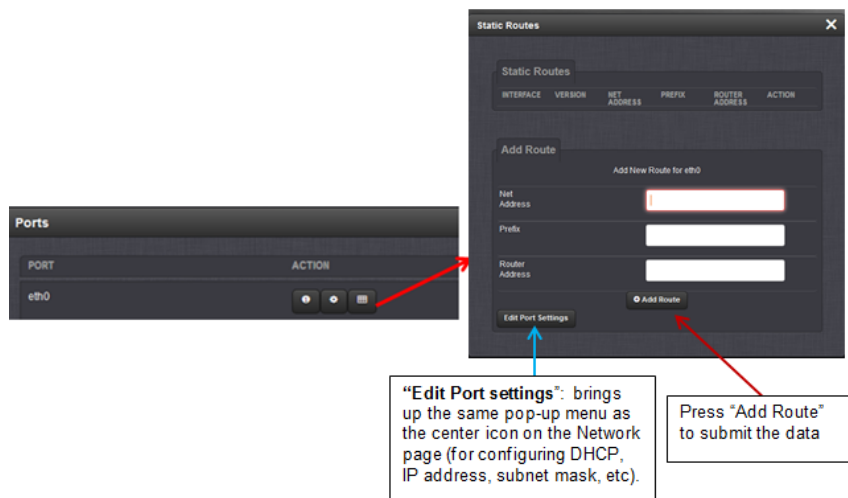
- **rt6add**: Adds an IPv6 static route.
- **rt6del**: Deletes IPv6 static route.
- **rt6get**: Displays the configured IPv6 routes.
- **routes6**: Displays the current IPv6 routing table(s)

### Configuring IPv4 static routes

- Static routes can be configured via ether:
  - The newer browser (refer to “A” below):
  - The CLI interface (refer to “B” below):

### B) Configuring IPv4 static routes using newer web browser (software versions 5.1.2 and above):

1. Navigate to the Management -> Network page of the browser
2. Click on the third (“table”) icon for the applicable eth0, eth1, eth2 or eth3 interface port that it’s desired to add the route.
3. In the “Add Route” pop-up window that opens, enter the **static route**
  - **Net Address**: This is the address/subnet to route to.
  - **Prefix**: This is the subnet mask in prefix form e.g., "24". See also [Subnet Mask Values](#).
  - **Router Address**: This is the gateway address the packet will initially go through to get there.
4. press “Add Route”.



### Fields:

- **Net Address**: (“This is the address/subnet to route to”, such as **10.2.0.0** for instance). For example, enter: “**10.10.1.101**” in this field). Note that the SecureSync doesn’t care how to get to this address after its sent to its gateway address
- **Prefix**: This is the subnet mask in prefix form (a two digit number for the subnet mask. Example: for a 255.255.255.0 subnet mask, enter “**24**” in this field). Refer to the table below to determine the applicable subnet mask’s two digit number:



| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

- **Router Address:** (“This is where you will go through to get there”) This is the IPv4Gateway address.
1. The entered info should now be displayed at the top of this pop-up menu.

### C) Configuring IPv4 static route using CLI interface (instead of the web browser)

**Note: (based on comment from Ron Dries)** I believe 5.1J update added ability to both edit and view routes via CLI. Previous versions only allowed static routes to be viewed in the cli.

From page 11-3 of the SecureSync Rev Q manual

|         |                                             |
|---------|---------------------------------------------|
| routes4 | Displays the current IPv4 routing table(s). |
| rt4add  | Adds an IPv4 static route.                  |
| rt4del  | Deletes an IPv4 static route.               |
| rt4get  | Displays the configured IPv4 static routes. |

From table above: **Rt4get rtbl** (where **rtbl** = the following routing tables)

M=main routing table

0= eth0 routing table

1= eth1 routing table

2= eth3 routing table

3= eth3 routing table

**Note:** The full syntax of each of these listed commands above can be obtained by typing the name of the command, followed by <enter>. For example, here is the result of typing **rt4add** <enter>, to add a new static route.

```
spadmin@Spectracom176 ~ $ rt4add
Invalid arguments
Usage: rt4add <rtbl> <nwcidr> <rtaddr>
  rtbl:  0=eth0, 1=eth1, etc.
  nwcidr: Network IPv4 CIDR, ie. 192.168.1.0/24
  rtaddr: Router IPv4 address, ie. 10.10.1.1
spadmin@Spectracom176 ~ $
```

## CLI command to retrieve/view the Ipv4 routing tables

Main default routing table: `ip route list table main <enter>`

```
[spadmin@Spectracom ~]$  
[spadmin@Spectracom ~]$ ip route list table main  
10.2.0.0/16 dev eth0 proto kernel scope link src 10.2.100.20  
10.2.0.0/16 dev eth3 proto kernel scope link src 10.2.100.94  
default via 10.2.1.1 dev eth0  
[spadmin@Spectracom ~]$
```

SRC= assigned IP address for that particular port

Eth0 routing table: `ip route list table t0 <enter>`

```
default via 10.2.1.1 dev eth0  
[spadmin@Spectracom ~]$ ip route list table t0  
10.2.0.0/16 dev eth0 scope link src 10.2.100.20  
default via 10.2.1.1 dev eth0  
[spadmin@Spectracom ~]$
```

Eth0 routing table: `ip route list table t0 <enter>`

Eth1 routing table: `ip route list table t1 <enter>`

Eth2 routing table: `ip route list table t2 <enter>`

Eth3 routing table: `ip route list table t3 <enter>`

---

### Reasons the static route may not have been created after pressing Submit

The static route has already been created.

- 1) The configured "router address" is not reachable from any Ethernet interface

---

### Deleting static routes

- Associated Log entry from Journal log: "requesting route for eth1 to be deleted."
- The "router address" must still be reachable in order to delete the static address. Otherwise, the static route won't be deleted.
  - **Example I used** - I unplugged eth1 from the network and then tried to delete a static route on Eth1. Route was not deleted. In v5.6.0, no error message was displayed.

### Can't delete static routes: "Error (512) on eth0 FAILURE detected in deleting route.. (SYSAL)"

|                    |         |                                                                  |
|--------------------|---------|------------------------------------------------------------------|
| May 17<br>19:20:27 | [WEB]   | Failed to delete network access restriction (cyrustech)          |
| May 17<br>19:20:27 | [webui] | Error (512) on eth0 FAILURE detected in deleting route.. (SYSAL) |
| May 17<br>19:20:27 | [webui] | Error (512) on eth0 FAILURE detected in deleting route.. (SYSAL) |

- Refer to Salesforce case 25398
- Observed in update version 5.4.1

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

### Troubleshooting static routes

1. Were the static routes manually added? Or, were they brought in with a previously saved config bundle?
2. If a config bundle was loaded into the SecureSync to clone settings, was the saved config bundle obtained from another SecureSyncv at the same version? Or, was the other SecureSync at a different version when the file was

### Known Issues with static routes

#### A) Software versions 5.4.5 and below (applicable to IPv6 static routes only)

1. IPv6 main gateway cannot be seen or set.
  2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
  3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed.

**Email from Paul M (1 Mar 17) from case 25398** Note some work was done on Release 5.4.5 to correct issues like this Ron commented in SSS-49 below. The issue is that there was problems with handling these addresses in earlier versions that was fixed in 5.4.5, YOU CAN USE THE COMMAND LINE TO FIX THESE issues as indicated below.

IPv6 address when duplicate cannot be deleted and IPv6 main gateway does not display or cannot set.

Since they are running 5.4.1 the text below from SSS-49 may apply.

There are general IPv6 from web ui configuration and display issues.

1. IPv6 main gateway cannot be seen or set.
2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed.

Furthermore you cannot delete these addresses fully from the Web ui. You might delete from the IPv6 stack, but an failure on delete leaves them in the /etc/conf.d/net file which restores them on reboot.

ip6del command will delete them from the file.

You can detect duplicate addresses by ip addr show eth# and look for addresses with status dadfailed

#### B) Software version 5.3.1

##### Static routes aren't being restored upon reboot

- (Mantis case 3228, Salesforce case 20224)
- Fix to be included in the version 5.4.0 update (~ Mar 2016).

#### C) Software version 5.3.0

##### Static routes broken

- (Mantis cases 3115 and 3118) Software update version 5.3.0 broke static routing functionality. Routes are still configurable, but don't work.
- This issue was addressed in the version 5.3.1 update (~Dec 2015)

### Error messages/conditions associated with static routes

1) “v6: eth1: IPv6 duplicate address 2001:4888:a03:310a:c0:fee:0:3 detected!”

➤ Refer to Salesforce case 23679

**Email from Paul M (1 Mar 17) from case 25398** Note some work was done on Release 5.4.5 to correct issues like this Ron commented in SSS-49 below. The issue is that there was problems with handling these addresses in earlier versions that was fixed in 5.4.5, YOU CAN USE THE COMMAND LINE TO FIX THESE issues as indicated below.

IPv6 address when duplicate cannot be deleted and IPv6 main gateway does not display or cannot set.

Since they are running 5.4.1 the text below from SSS-49 may apply.

There are general IPv6 from web ui configuration and display issues.

1. IPv6 main gateway cannot be seen or set.
2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed.

Furthermore you cannot delete these addresses fully from the Web ui. You might delete from the IPv6 stack, but an failure on delete leaves them in the /etc/conf.d/net file which restores them on reboot.

ip6del command will delete them from the file.

You can detect duplicate addresses by ip addr show eth# and look for addresses with status dadfailed

## IPv6 static routes

Note: info regarding IPv4 static routes is further above in a separate section

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

### Software updates associated with IPv6 static routes

#### v5.7.3

- Updated IPv6 networking support to more closely match IPv4 networking. Added additional routing tables per network port with individual IPv6 default gateways. Static IPv6 routes can be applied per network port.
- Note: As of at least software update version 5.2.1, IPv6 static routes are only available for the configured main default gateway port only, (not available for the other network ports).

#### v5.2.0

Software update version 5.2.0 added basic **static IPv6 routing capability** by allowing manual configuration of IPv6 routes via CLI commands (not yet available via the web browser, as of at least version 5.2.1)

**Note:** an example of each command is below the table

| IPv6 (versions 5.2.0 and above) |                                             |
|---------------------------------|---------------------------------------------|
| <b>routes6</b>                  | Displays the current IPv6 routing table(s). |
| <b>rt6add</b>                   | Adds an IPv6 static route.                  |
| <b>rt6del</b>                   | Deletes an IPv6 static route.               |
| <b>rt6get</b>                   | Displays the configured IPv6 static routes. |

- **routes6:** Displays the current IPv6 routing table(s)

Usage: **rt6add** <nwcidr> <rtaddr>

**nwcidr:** Network IPv6 CIDR, ie. 2000::/64

**rtaddr:** Router IPv6 address, ie. 2001::1

- **rt6get:** Displays the configured IPv6 routes.
- **rt6add:** Adds an IPv6 static route.
- **rt6del:** Deletes IPv6 static route

Where:

- **<nwcidr>** is the IPv6 address (CIDR) for the main default gateway.
- **<rtaddr>** is the IPv6 address for the router

```
spadmin@Spectracom176 ~ $ routes6
Main routing table:
fe80::/64 dev eth0 proto kernel metric 256

spadmin@Spectracom176 ~ $ rt6add
Invalid arguments
Usage: rt6add <nwcidr> <rtaddr>
nwcidr: Network IPv6 CIDR, ie. 2000::/64
rtaddr: Router IPv6 address, ie. 2001::1

spadmin@Spectracom176 ~ $ rt6del
Invalid arguments
Usage: rt6del <nwcidr>
nwcidr: Network IPv6 CIDR, ie. 2000::/64

spadmin@Spectracom176 ~ $ rt6get
Main routing table:
```

## Troubleshooting customer's routes/static routes

**NOTICE:** IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise the config changes won't be accepted.

- Request a topographical diagram of the customer's network.
- Software update version 5.2.0 added basic static IPv6 routing capability by allowing manual configuration of IPv6 routes via CLI commands (not yet in web browser)
- (Mantis cases 3115 and 3118) Software update version 5.3.0 broke static routing functionality. Routes are still configurable, but don't work. Fixed in version 5.3.1.

## Configuration of IPv6 static routes

### A) Classic Interface web browser:

**Network -> General Setup** page, **General** tab (or via CLI interface)

**"Static Routes" table in this tab:** Used to define networks on other side of routers that are attached to any or all of the Ethernet ports (but are not available through the default gateway). "Network address" will likely end in 0's (don't include the / and bits to define the subnet mask. These are entered with just the number in the "Prefix field". Enter the router's IP address in the "Router Address" field.

In the example screenshot below, Eth 0 happens to have a router at 10.2.100.1 that is also attached to a 192.168.1.x network. And, it's desired for network traffic to be broadcasted to this other subnet.

| Network Bits | Equivalent Netmask | Network Bits | Equivalent Netmask |
|--------------|--------------------|--------------|--------------------|
| 30           | 255.255.255.252    | 18           | 255.255.192.0      |
| 29           | 255.255.255.248    | 17           | 255.255.128.0      |
| 28           | 255.255.255.240    | 16           | 255.255.0.0        |
| 27           | 255.255.255.224    | 15           | 255.254.0.0        |
| 26           | 255.255.255.192    | 14           | 255.252.0.0        |
| 25           | 255.255.255.128    | 13           | 255.248.0.0        |
| 24           | 255.255.255.0      | 12           | 255.240.0.0        |
| 23           | 255.255.254.0      | 11           | 255.224.0.0        |
| 22           | 255.255.252.0      | 10           | 255.192.0.0        |
| 21           | 255.255.248.0      | 9            | 255.128.0.0        |
| 20           | 255.255.240.0      | 8            | 255.0.0.0          |
| 19           | 255.255.224.0      |              |                    |

Table 2.3. Subnet mask table

| Static Routes |            |                 |        |                |                          |
|---------------|------------|-----------------|--------|----------------|--------------------------|
| Interface     | IP Version | Network Address | Prefix | Router Address | Delete                   |
| eth0          | IPv4       | 192.168.1.0     | 24     | 10.2.100.1     | <input type="checkbox"/> |
| eth0          | IPv4       |                 | 0      |                | <input type="checkbox"/> |
| eth0          | IPv4       |                 | 0      |                | <input type="checkbox"/> |
| eth0          | IPv4       |                 | 0      |                | <input type="checkbox"/> |
| eth0          | IPv4       |                 | 0      |                | <input type="checkbox"/> |

**Note (as of 3/28/13) about IPv6 Static Routes:** IPv4 Static Routes are supported. IPv6 Static Routes are **not** currently supported (Refer to Mantis case 1936/1937 <http://cvsmantis.int.rolia.com/mantis/view.php?id=1937> ). The drop-downs only allow IPv4 to be selected (this is beyond just adding a new value to the drop-down).

**Email from Dave Sohn regarding the intentions to add IPv6 Static Routes (28 March 2013)** In my response to the issues presented by Roots I presented the resolution of some issues and feature requests. IPv6 gateway support fix was included, but IPv6 routing was not. IPv6 routing requires some extensive development similar to getting the multiple interface IPv4 routing to work we did a few years ago. It is in our sustaining plan to add this, but is dependent on resources, which are allocated elsewhere at this time. I hope to get something into our end of Q3 or Q4 release, but that is still dependent on resource availability.

---

## Issues/software changes associated with IPv6 static routes

- Refer also to “Issues with IPv4/IPv6 Static routes” further above in the “IPv4 static routes” section

**Email from Paul M (1 Mar 17) from case 25398** Note some work was done on Release 5.4.5 to correct issues like this Ron commented in SSS-49 below. The issue is that there was problems with handling these addresses in earlier versions that was fixed in 5.4.5, YOU CAN USE THE COMMAND LINE TO FIX THESE issues as indicated below.

IPv6 address when duplicate cannot be deleted and IPv6 main gateway does not display or cannot set.

Since they are running 5.4.1 the text below from SSS-49 may apply.

There are general IPv6 from web ui configuration and display issues.

1. IPv6 main gateway cannot be seen or set.
2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed. Furthermore you cannot delete these addresses fully from the Web ui. You might delete from the IPv6 stack, but an failure on delete leaves them in the /etc/conf.d/net file which restores them on reboot.

ip6del command will delete them from the file.

You can detect duplicate addresses by ip addr show eth# and look for addresses with status dadfailed

---

## \*\*Network troubleshooting in SecureSync (tcpdump, ping, arp, traceroute/tracepath, etc)

- Refer to Mantis case 1583 for more details.

---

### TCPdump (wireshark for Linux)

- TCPdump is a command line packet capture tool (these captures can be opened with wireshark)  
**Note:** includes the ability to delete tcpdump via web browser, if desired. See additional info below.

#### Software version changes associated with tcpdump

##### 1. (v5.7.3 update): tcpdump was updated to 4.9.2 to resolve many vulnerabilities:

- CVE-2017-11108, CVE-2017-(11541-11544), CVE-2017-(12893-12902), CVE-2017-(12985-13055), CVE-2017-(13687-13690), CVE-2017-13725

##### 2. Other previous SecureSync version changes associated with tcpdump

- tcpdump was temporarily available with patch version 4.8S installed.
- 4.8S can be installed on any version 4.8.x release to add tcpdump.
- If updated to at least 5.0.0 or 5.0.1 tcpdump will no longer be available
- tcpdump was added back in via update software version 5.2.1 (May 2015)

---

### Location of TCPdump in the system

- tcpd (tcpdump) is in the **home/spectracom/usr/sbin** directory

---

### Disabling TCPDump (if desired)

**Note:** If tcpdump **responds with a password** (as shown below) tcpdump has been disabled (and cant be re-enabled without performing a full update/restore to default)

```
spadmin@Spectracom:~  
login as: spadmin  
Using keyboard-interactive authentication.  
Password:  
tSpectracom NetClock 9483 Version 5.7.1  
spadmin@Spectracom ~ $ tcpdump  
Password: █
```

TCPdump can be disabled in the bottom-left corner of the **Management -> Network** pages via a slider switch (under **"Network Services"**). Once deleted, it can only be brought back with a "restore to factory defaults" update (It's not restored just by performing a "clean" or by updating the software to a newer version). See additional info below.

#### (Software issue in v5.9.4) Can't disable tcpdump

- refer to Salesforce case 281483 and JIRA SSS-1253

**Report from customer:** I'm attempting to disable tcpdump on our 1200-011, running System Orolia SecureSync SW V5.9.4. I get a message saying tcpdump will be permanently removed, I hit okay, and I get two messages. First I get tcpdump removed, but next I get "405: method not allowed". If I refresh the page, tcpdump is back and enabled. I tried rebooting it from the web console but it still has the same issue.

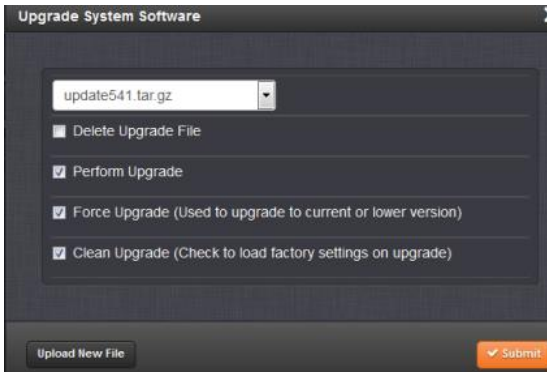


## Re-enabling tcpdump once it's been "disabled" in the system

To begin, tcpdump is available for use, by factory default, in SecureSync software versions 5.2.1 and above. Tcpdump remains available for use until its "permanently" disabled via the "tcpdump" slider switch in the **Management** -> **Network** page of the browser. Unlike other Services which can be disabled/re-enabled as desired, for security purposes, tcpdump availability is removed from the system once it's been changed to disabled. Once the tcpdump slider switch has been moved, this service is no longer available until a "Clean Upgrade" (not just a "clean" command) has been performed.

To restore tcpdump once it's been disabled, perform a **"Clean Upgrade"**, Note this will reset all the unit's configurations back to the factory default settings for the version of software being applied during this process (the same version of software can be re-applied to keep it the same version, as desired).

The start of this process is similar to performing a standard software update to the latest version. But after selecting/uploading the software update bundle into the SecureSync, instead of just selecting the **"Perform Upgrade"** checkbox, both the **"Force Update"** and **"Clean Upgrade"** checkboxes also need to be selected, as well (as shown below). Then press Submit.



Once the "Clean Upgrade" process has been completed, the unit can then be reconfigured as desired and TCPdump will be available for use again (until the slider bar for TCPdump is changed to disabled again).

If you wish to remain at the current version already installed in the SecureSync, you just use the update bundle for this particular software version (such as version 5.7.1 for instance). It doesn't hurt anything to re-install the same version that is already installed. Or, you can alternatively download the latest version of software and update the software to the latest rev, at the same time. Whichever you prefer,

Attached for your reference is a copy of the standard software update instructions for version 5.8.4 (the latest version for SecureSync) To apply the version 5.8.4 software for example (either to keep it at version 5.8.4 or to upgrade it to version 5.8.4 from an earlier version, as we always recommend having the latest version of software installed), the version 5.8.4 software update bundle can be downloaded from our website. Here is the link to download the version 5.8.4 update bundle and upgrade instructions: <https://files.spectracom.com/public-downloads/update-files-securesyncnetclock-9400-version-584>

Follow the update instructions up to the point where it indicates to select **"Perform Upgrade"**, but then **ALSO** select the other two checkboxes referenced above (both the **"Force Update"** and **"Clean Upgrade"** checkboxes). Then press Submit. Once the update has completed, the unit will have been restored to its factory default settings and tcpdump will be available again.

## Applying a previously saved config bundle after performing a "Restore to Defaults" process

- the config bundle stores whether or not to disable tcpdump if the bundle is applied
- refer to info further below on how to tell whether a bundle will disable tcpdump if its applied.

Email Keith sent (19 March 2019) Unless you know whether the backup config file was created either before or after tcpdump was disabled/deleted, we don't recommend using the saved file to restore the unit after performing the "restore to defaults".

If this file was generated/created before tcpdump was originally removed, tcpdump will remain available after applying the file. But if the config file was generated after tcpdump was disabled, restoring the config file will disable it again (thereby requiring you to repeat the same restore to defaults process again to re-enable it).

If you aren't sure the exact order of sequence of when the config bundle file was generated vs when tcpdump was disabled, and you decide to apply the config bundle after the restore to defaults, you essentially have a 50/50 chance that you may have to repeat the process after restoring the configs.

To prevent potentially having to perform the restore to defaults a second time, we recommend manually restoring the configs, this time. Then replace the previously saved config file with a new one having tcpdump still available.

By the way, I JUST found some info on how to tell whether the bundle will remove tcpdump, if its applied.

Make a copy of the bundle file, and then extract the copy file (using a program such as “7-zip” for tar files). Then go to the **/config** folder in the bundle.

There is a **remove.conf** file in this folder, which determines if tcpdump is to be removed when the bundle is applied:

- If tcpdump wasn't yet removed when the file was generated, this file will be empty (tcpdump will remain useable after applying the file)
- If tcpdump had been removed when the bundle was generated, this file will contain: “usr/sbin/tcpdump” (tcpdump will again be removed after applying the file).

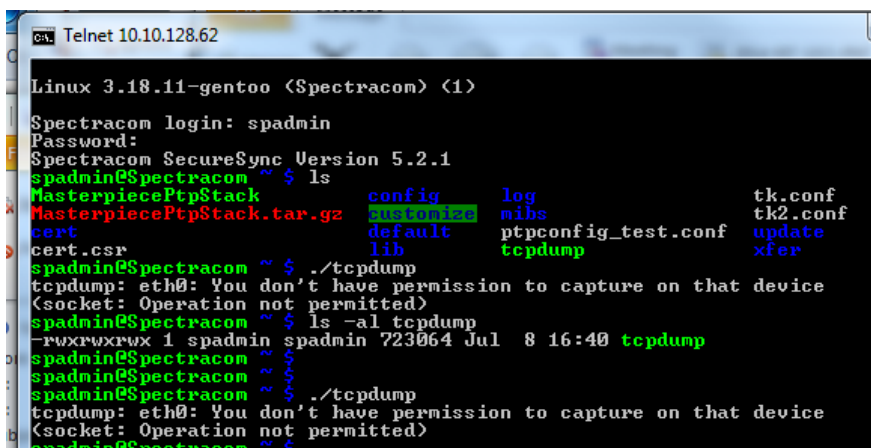
---

### Configuration of whether TCPDump has been removed from the system

- The setting of whether TCPDump has been removed is in the **remove.conf** file (located in the **/config** file)
  - If not yet removed, this file will be empty
  - If TCPDump has been removed, this file will contain: “usr/sbin/tcpdump”

**Ability for a “user” to install tcpdump into SecureSync to be able to capture network traffic (i.e. if an admin has already removed tcpdump for security reasons)**

**Per Paul Myers (7 jul 15)** You can't get access to underlying features using spadmin owned tcpdump (note from Keith- Paul had a co-op remove TCPDump using the slider switch and then brought it back into the system using spadmin. This shows a user can't simply install tcpdump and start using it with just admin rights (must use the default tcpdump or be logged in as a root to use a different tcpdump.



```
ca. Telnet 10.10.128.62
Linux 3.18.11-gentoo <Spectracom> <1>
Spectracom login: spadmin
Password:
Spectracom SecureSync Version 5.2.1
spadmin@Spectracom ~ $ ls
MasterpiecePtpStack  config          log             tk.conf
MasterpiecePtpStack.tar.gz  default        mibs           tk2.conf
cert                lib            ptpconfig_test.conf  update
cert.csr            tcpdump       xfer
spadmin@Spectracom ~ $ ./tcpdump
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
spadmin@Spectracom ~ $ ls -al tcpdump
-rwxrwxrwx 1 spadmin spadmin 723064 Jul  8 16:40 tcpdump
spadmin@Spectracom ~ $ ./tcpdump
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
spadmin@Spectracom ~ $
```

---

### Network “Access Control” and ability to run TCPdump

- TCPdump requires access to a command prompt (Telnet or SSH) in order to run.
- If Network “Access Control” has been established (limiting access to Services by IP addresses) and a user on a PC that is not on the Access list tries to “sniff” the network, they won't be able to connect with telnet or ssh in order to run tcpdump.

**Email from Keith to a customer (8 July 2015)** Sniffing the network traffic requires a unique tool be installed on the machine (TCPdump for Linux or a program such as wireshark for Windows). Prior to version 5.2.0 software in SecureSync, none of

these type programs were available on SecureSync. But TCPdump was added to SecureSync in version 5.2.0 for customers that want to be able to view the raw SecureSync packets from within the SecureSync.

For customers that don't want TCPDump to be available (note it can only be run from the CLI command prompt and can't be run from the web browser) it can be disabled from the Management -> Network page of the browser (there is a slider switch for it on the left side). Once it's been disabled by a user, even performing a "clean" or updating the software to a newer version will enable it again (the other slider switches for each of the other Services listed on this page can be disabled and re-enabled whenever desired). The only way to re-enable tcpdump once it's been disabled is to perform a "restore to factory default settings". Once it's been disabled, it can't be run from any network port, even if the Access Control list remains empty.

In order to run this utility (as long as it hasn't been disabled yet), a user logs into Telnet or SSH to establish a command line interface with the SecureSync. In order to connect via either telnet or SSH, a user account and password has to be known. With no IP addresses in the Network Access Control list, a user can try to connect to telnet or ssh and will get a login prompt. If they know a valid username and password, they can connect and run tcpdump. But if the Access Control List is used to limit access to all Services, and someone tries to connect to the CLI from a machine that isn't allowed in this Access list, they will not even be able to get to the telnet or SSH login screen. Even if they have a valid username and password, they won't be able to connect to any of the Services (telnet, SSH, FTP, web browser, etc). Since they won't be able to reach any of the Services to even attempt to connect, they can't run tcpdump or any other utility that can be used to sniff the network packets. If the machine's address isn't in the access list to allow it, they can only sync their PC with NTP time stamps.

In summary, the Access list blocks access to the ability for all unauthorized machines to be able to open a command prompt, which is needed to run the tcpdump program that is used to sniff the network ("not authorized" IP addresses can only obtain NTP time stamps for network time synchronization - note that even this capability can be blocked if desired, because NTP has its own access control available, as well).

---

## Using TCPdump (versions 5.2.0 and above)

### Need to use a mirrored port (port mirroring) on switches

- Applicable to unicast packets only (not applicable to multicast)
- Switches direct traffic to the appropriate port only, so packets not meant for other ports aren't router to that port
- Won't be able to capture packets unless on the same port or traffic is also directed to another port as well (this is port mirroring)
- Some, but not all switches support port mirroring.

### Desire to use TCPdump to capture PTP traffic

- TCPdump can be used to capture PTP traffic that is on the same network as eth0, eth1, eth2 or eth3.
- TCPdump cannot be used to capture PTP traffic if the PTP Master and PTP Slaves are on their own dedicated network.

**Email from Keith (9 Sept 16)** As the PTP cards and the SecureSync's Ethernet ports are internally not on the same network, and as both the PTP Master and slaves need to be involved in the capture, you can't just loop a PTP connection over to any of the standard network ports to perform a capture.

The only way to use the SecureSync to perform a PTP packet capture is to connect one of its standard Ethernet interfaces (eth0 - eth3) to a mirrored port on the switch (making one of the SecureSync' Ethernet interfaces act like a PC on the same switch). Then run tcpdump in the SecureSync's CLI interface by typing: `sudo tcpdump <enter>`.

Refer to tcpdump info online on how to use this program: sites such as [http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html) or <https://danielmiessler.com/study/tcpdump/>

For example, **sudo tcpdump -i eth1** will capture the traffic on eth1 (instead of the default port of eth0).

To capture just PTP packets on Eth0: **sudo tcpdump port 319 and 320**

To capture all traffic to a File `sudo tcpdump -w securesync .pcap`

Note the file is created/stored in the home/spectracom directory (FTP it out from this directory).

Control + c stops the capture.

## Running/using tcpdump

### Notes:

- 1) use **CTRL + C** to stop a capture in progress
- 2) If the tcpdump command **responds with a password** (as shown below) tcpdump has been disabled in the time sever (and can't be re-enabled without performing a full upgrade/restore to factory default)

```
spadmin@Spectracom:~  
login as: spadmin  
Using keyboard-interactive authentication.  
Password:  
tSpectracom NetClock 9483 Version 5.7.1  
spadmin@Spectracom ~ $ tcpdump  
Password: █
```

### CLI Command:

#### 1. Versions 5.4.5 and above:

- **tcpdump** (starting in v5.4.5, spadmin now has rights to run tcpdump. No longer need to issue **sudo** to run it)

#### 2. Versions 5.4.1 and below:

- **sudo tcpdump** (details below)
- Tcpdump can only be run from a command prompt (telnet or ssh). It cannot be run from the web browser

**Note:** tcpdump is not in helpcli.

- Refer to normal tcpdump info on how to use this program- sites such as [http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html) or <https://danielmiessler.com/study/tcpdump/>

**Notice:** (versions 5.4.1 and below) tcpdump MUST be run as **sudo** (type **sudo** before also typing **tcpdump**)

- If you type just tcpdump without **sudo** in front, it will respond with **Permission denied**.

### Login as spadmin and type either:

- Versions 5.4.5 and above: **tcpdump** <enter>
- Versions 5.4.1 and below: **sudo tcpdump** <enter>

**Note:** omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

### Ethernet interface data is captured on (eth0 is the default)

Unless one or more ports are specified, the default is to listen on Eth0 only. To listen on a port other than eth0, after tcpdump type -i (lower case, like in india) followed by **eth1 eth2** or **eth3**

### Examples

To capture data on specific (or all) Ethernet interfaces

Note-omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE

- To capture traffic on **eth1** instead of eth0: **sudo tcpdump -i eth1**
- To capture traffic on more than one interface (such as eth0 and eth1): **sudo tcpdump -i eth0 -i eth1**
- To capture traffic on all interfaces (eth0 thru eth 3): **sudo tcpdump -i any**

To capture specific data type of packets (such as Radius packets only, snmp only)

Note-omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE

- **NTP** on eth0: **sudo tcpdump port 123** (no need to define interface as eth0 is default)
- **Radius** on eth0: **sudo tcpdump port 1812 and 1813** (no need to define interface as eth0 is default)
- **LDAP** on eth0: **sudo tcpdump port 389 and 636** (no need to define interface as eth0 is default)
- **Syslog** on eth0: **sudo tcpdump port 514** (no need to define interface as eth0 is default)
- **PTP** on eth0: **sudo tcpdump ports 319 and 320** (no need to define interface as eth0 is default)
- **SNMP gets** on eth0: **sudo tcpdump port 161** (no need to define interface as eth0 is default)
- **SNMP Traps** sent to any Ethernet interface: **sudo tcpdump port 162 -i any**

```
spadmin@Spectracom ~ $ sudo tcpdump port 162 -i any
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
21:20:11.907881 IP 10.2.100.176.52835 > roc-ops-kwing.int.oroilia.com.snmptrap: C="snmptrap
" V2Trap(81) system.sysUpTime.0=269581 S:1.1.4.1.0=E:18837.3.2.3.0.2 E:18837.3.2.2.1.6.0=1
21:20:11.942491 IP 10.2.100.176.52835 > roc-ops-kwing.int.oroilia.com.snmptrap: C="snmptrap
" V2Trap(101) system.sysUpTime.0=269584 S:1.1.4.1.0=E:18837.3.2.3.0.12 E:18837.3.2.2.1.3.0
=" " E:18837.3.2.2.1.4.0=""
^C
2 packets captured
```

To stop a capture and exit tcpdump Use: **Control + C**

To highlight specific words, type: **sudo tcpdump | grep xxxxx**

To be able to scroll through packets: **sudo tcpdump | less**

Then: Press “/” followed by letter(s) to highlight the letters in all of the packets

(press **q** to exit out of the view)

## Options

Note-omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE

- 1) **Basic communication** // see the basics without many options **sudo tcpdump -nS <enter>**
- 2) **Basic communication (very verbose)** // see a good amount of traffic, with verbosity and no name help : **sudo tcpdump -nnvVS <enter>**
- 3) **A deeper look at the traffic** // adds -X for payload but doesn't grab any more of the packet  
**sudo tcpdump -nnvXS <enter>**
- 4) **Heavy packet viewing** // the final “s” increases the snaplength, grabbing the whole packet  
**sudo tcpdump -nnvXSs 1514 <enter>**

There are three main types of expression: type, dir, and proto.

**Note: omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE**

**Type** options are **host**, **net**, and **port**. Direction is indicated by **dir**, and there you can have **src**, **dst**, **src or dst**, and **src and dst**. Here are a few that you should definitely be comfortable with:

- **host** // look for traffic based on IP address (also works with hostname if you're not using **-n**)  
**sudo tcpdump host 1.2.3.4**
- **src, dst** // find traffic from only a source or destination (eliminates one side of a host conversation)  
**sudo tcpdump src 2.3.4.5**  
**sudo tcpdump dst 3.4.5.6**
- **net** // capture an entire network using [CIDR](#) notation  
**sudo tcpdump net 1.2.3.0/24**
- **proto** // (works for tcp, udp, and icmp). Note that you don't have to type proto  
**sudo tcpdump tcp**  
**sudo tcpdump udp**  
**sudo tcpdump i**
- **port** // see only traffic to or from a certain port  
**sudo tcpdump port xxx (where xxx is the desired port number to listen for)**
- **src, dst port** // filter based on the source or destination port  
**sudo tcpdump src port 1025 # tcpdump dst port 389**
- **src/dst, port, protocol** // combine all three  
**sudo tcpdump src port 1025 and tcp**  
**sudo tcpdump udp and src port 53**
- You also have the option to filter by a range of ports instead of declaring them individually, and to only see packets that are above or below a certain size.

## SYNOPSIS

**tcpdump** [ **-AbdDefhHIJKILnNOPqRStuUvxX#** ] [ **-B** *buffer\_size* ]

[ **-c** *count* ]

[ **-C** *file\_size* ] [ **-G** *rotate\_seconds* ] [ **-F** *file* ]

[ **-i** *interface* ] [ **-j** *tstamp\_type* ] [ **-m** *module* ] [ **-M** *secret* ]

[ **--number** ] [ **-Q** *in|out|inout* ]

[ **-r** *file* ] [ **-V** *file* ] [ **-s** *snaplen* ] [ **-T** *type* ] [ **-w** *file* ]

[ **-W** *filecount* ]

[ **-E** [spi@ipaddr](#) *algo:secret,...* ]

[ **-y** *datalinktype* ] [ **-z** *postrotate-command* ] [ **-Z** *user* ]

[ **--time-stamp-precision=***tstamp\_precision* ]

```
[ --immediate-mode ] [ --version ]  
[ expression ]
```

## Options

Below are a few options (with examples)

First off, I like to add a few options to the tcpdump command itself, depending on what I'm looking at. The first of these is **-n**, which requests that names are not resolved, resulting in the IPs themselves always being displayed. The second is **-X**, which displays both hex and ascii content within the packet. The final one is **-S**, which changes the display of sequence numbers to absolute rather than relative. The idea there is that you can't see weirdness in the sequence numbers if they're being hidden from you. Remember, the advantage of using tcpdump vs. another tool is getting manual interaction with the packets.

It's also important to note that tcpdump only takes the first 96 bytes of data from a packet by default. If you would like to look at more, add the **-s number** option to the mix, where *number* is the number of bytes you want to capture. I recommend using 0 (zero) for a snaplength, which gets everything. Here's a short list of the options I use most:

- **-i any** : Listen on all interfaces just to see if you're seeing any traffic.
  - **-n** : Don't resolve hostnames.
  - **-nn** : Don't resolve hostnames *or* port names.
  - **-X** : Show the packet's *contents* in both hex and ASCII.
  - **-XX** : Same as **-X**, but also shows the ethernet header.
  - **-v, -vv, -vvv** : Increase the amount of packet information you get back.
  - **-c** : Only get x number of packets and then stop.
  - **-s** : Define the *snaplength* (size) of the capture in bytes. Use -s0 to get everything, unless you are intentionally capturing less.
  - **-S** : Print absolute sequence numbers.
  - **-e** : Get the ethernet header as well.
  - **-q** : Show less protocol information.
  - **-E** : Decrypt IPSEC traffic by providing an encryption key.
- **Port Ranges** // see traffic to any port in a range  
tcpdump **portrange 21-23**
  - **Packet Size Filter** // only see packets below or above a certain size (in bytes)  
tcpdump **less 32**  
tcpdump **greater 128**

[You can use the symbols for less than, greater than, and less than or equal / greater than or equal signs as well. ]  
// filtering for size using symbols

```
tcpdump > 32  
tcpdump <= 128
```

---

## Writing to a File

- tcpdump allows you to send what you're capturing to a file for later use using the -w option, and then to read it

back using the -r option. This is an excellent way to capture raw traffic and then run it through various tools later.

The traffic captured in this way is stored in tcpdump format, which is pretty much universal in the network analysis space. This means it can be read in by all sorts of tools, including [Wireshark](#), [Snort](#), etc.

### Capture all traffic to a File

**Note: omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE**

- The file is created/stored in the home/spectracom directory.

**sudo tcpdump -w securesync .pcap**

**Note:** securesync.pcap below is an arbitrary file name used as an example (Can name the file as desired).

Then, at some point in the future, you can then read the traffic back in like so: **Read Captured Traffic back into tcpdump**

**sudo tcpdump -r secureSync.pcap**

---

### Log entries associated with tcpdump

#### Auth.log

- No auth log entries are asserted when starting tcpdump normally.

#### Trying to start tcpdump using “su” instead of “sudo” (or just typing “tcpdump” by itself)

- Note the correct command to start tcpdump is “**sudo tcpdump**”

```
su[8096]: pam_unix(su:auth): authentication failure; logname=spadmin uid=1002 euid=0 tty=/dev/pts/2 ruser=spadmin rhost=
user=tcpdump
```

```
su[8096]: FAILED su for tcpdump by spadmin su[8096]: - /dev/pts/2 spadmin:tcpdump
```

#### System log

**Two entries asserted when logging into the classic interface browser with versions 5.2.0 and above.**

```
Aug 3 15:10:57 custservice176 custservice176: [spadmin] ERROR (2) - Error SEC_GetGroup (username[0,1]=quagga) (WEB)
```

```
Aug 3 15:10:57 custservice176 custservice176: [spadmin] ERROR (2) - Error SEC_GetGroup (username[1,2]=tcpdump)
(WEB)
```



---

## Available CLI commands for troubleshooting network issues (ping, traceroute, dig, etc)

Starting in SecureSync software version 4.8.0, customers will be able to troubleshoot network issues from within SecureSync (instead of just external to the SecureSync). There are several tools being added to provide standard Linux commands for troubleshooting the network traffic. These commands are only available in the CLI port (not on the web browser) and are intended for experienced users only.

### The added commands are:

Ping, ifconfig, arp, rarp, route, netstat, domainname, dig, host, nslookup, traceroute

To use these commands, login with any CLI connection (Serial port, telnet or ssh). Then, type these commands at the command prompt.

**Note:** Pressing **CTRL / C** can be used to end the command (for commands like ping which will keep going until CTRL and C are pressed together)

### Ping

- type ping followed by IP address of the other device you wish to ping)

**Function:** Can ping another network device FROM the NTP server. Note that it will continue to ping until press **CTRL / C**.

---

### Routes/Routing tables for the network ports

**Note:** Software update version 5.2.0 added basic static IPv6 routing capability by allowing manual configuration of IPv6 routes via CLI commands (not yet in browser)

- Refer also to routing tables further below in the network section of this document
- Route: (just type **"route"**)

**Function:** manipulates the kernel's IP routing tables. Its primary use is to **set up static routes** to specific hosts or networks via an interface after it has been configured with the **ifconfig** program.

**Note:** Can VIEW routing tables, but not CONFIGURE via CLI (note this may have since changed)

```
[spadmin@Spectracom ~]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.2.0.0 * 255.255.0.0 U 0 0 0 eth0
default 10.2.1.1 0.0.0.0 UG 0 0 0 eth0
[spadmin@Spectracom ~]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.2.0.0 * 255.255.0.0 U 0 0 0 eth0
default 10.2.1.1 0.0.0.0 UG 0 0 0 eth0
[spadmin@Spectracom ~]#
[spadmin@Spectracom ~]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.2.0.0 * 255.255.0.0 U 0 0 0 eth0
default 10.2.1.1 0.0.0.0 UG 0 0 0 eth0
[spadmin@Spectracom ~]#
```

Main default routing table: **ip route list table main** <enter>

```
[spadmin@Spectracom ~]$  
[spadmin@Spectracom ~]$ ip route list table main  
10.2.0.0/16 dev eth0 proto kernel scope link src 10.2.100.20  
10.2.0.0/16 dev eth3 proto kernel scope link src 10.2.100.94  
default via 10.2.1.1 dev eth0  
[spadmin@Spectracom ~]$
```

SRC= assigned IP address for that particular Ethernet interface

Eth0 routing table: **ip route list table t0** <enter>

```
default via 10.2.1.1 dev eth0  
[spadmin@Spectracom ~]$ ip route list table t0  
10.2.0.0/16 dev eth0 scope link src 10.2.100.20  
default via 10.2.1.1 dev eth0  
[spadmin@Spectracom ~]$
```

Eth1 routing table: **ip route list table t1** <enter>

Eth2 routing table: **ip route list table t2** <enter>

Eth3 routing table: **ip route list table t3** <enter>

## tracpath and traceroute commands

- The command used to be “traceroute”. Has since been changed to “tracpath” in at least v5.4.1 (traceroute is no longer a valid command. Not sure in which software update this change occurred).

**Function:** Shows the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes

### A) Traceroute

- **Note:** it appears *tracpath* command may no longer work in at least 5.8.2 (if not earlier, also)
  - IPv4 or IPv6: Type “**traceroute** followed by the destination address.
- Refer to sites such as: <https://www.geeksforgeeks.org/traceroute-command-in-linux-with-examples/>

Below image depicts how traceroute command is used to reach the Google(172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.

```
prabhakar@inspiron-3542:~$ traceroute google.com  
traceroute to google.com (172.217.26.206), 30 hops max, 60 byte packets  
 1 192.168.43.45 (192.168.43.45) 2.014 ms 2.313 ms 2.588 ms  
 2 * * *  
 3 10.45.1.230 (10.45.1.230) 75.449 ms 115.244 ms 115.224 ms  
 4 10.45.8.178 (10.45.8.178) 93.856 ms 115.138 ms 93.822 ms  
 5 10.45.8.187 (10.45.8.187) 115.116 ms 115.106 ms 115.070 ms  
 6 * * *  
 7 218.248.235.141 (218.248.235.141) 120.589 ms 108.033 ms 106.962 ms  
 8 218.248.235.142 (218.248.235.142) 114.489 ms * *  
 9 72.14.211.114 (72.14.211.114) 98.076 ms 93.232 ms 93.781 ms  
10 108.170.253.113 (108.170.253.113) 98.688 ms 91.388 ms 108.170.253.97 (108.170.253.97) 107.241 ms  
11 74.125.253.69 (74.125.253.69) 95.120 ms 72.14.237.165 (72.14.237.165) 102.594 ms 103.137 ms  
12 maa03s23-in-f14.1e100.net (172.217.26.206) 101.794 ms 97.987 ms 97.165 ms  
prabhakar@inspiron-3542:~$
```

The first column corresponds to the hop count. The second column represents the address of that hop and after that, you see three space-separated time in milliseconds. `traceroute` command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop.

By default `traceroute` sends three packets for each host so three response times are listed.

If an **asterisk** is here, it means there wasn't a response for that test. If the device doesn't respond at all, you'll see three asterisks, and no device name or IP address.

In this example the asterisks show packet loss. This could mean a network outage, high amounts of traffic leading to network congestion or a firewall dropping traffic. Whatever the reason the `traceroute` command shows the destination is not reached.

The following example shows a `traceroute` that fails to reach the destination.

```
traceroute google.com
traceroute to google.com (172.217.25.46), 30 hops max, 60 byte packets
 1 10.8.8.1 (10.8.8.1) 316.212 ms 316.393 ms 317.031 ms
 2 107.181.128.1 (107.181.128.1) 322.328 ms 326.666 ms 326.4
 3 au-sy3-bdr-0-0.as58940.net.au (43.245.167.1) 321.205 ms 3
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 ...
```

- This command works for both IPv4 or IPv6 (the `-4` or `-6` switch can be added to force one or the other, but this isn't necessary).

```
traceroute to 10.2.100.35 (10.2.100.35), 30 hops max, 40 byte packets
 1 10.2.100.35 (10.2.100.35) 1.275 ms 0.326 ms 0.268 ms
 [spadmin@Spectracom ~]$
```

### traceroute using a specified port number (such as port 123)

- Switch `-p` allows a desired port number to be specified

`traceroute -p 123 time.spectracomcorp.com` As shown below, verify the last value is **74.112.39.70** followed by **"reached"** at the end of the line:

```
Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
1?: [LOCALHOST] pmtu 1500
 1: 10.2.1.1 2.353ms
 1: 10.2.1.1 2.239ms
 2: 74.112.39.70 2.165ms reached
Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

### Example of a destination address not being available via port 123 ("send failed" to a bad address)

```
spadmin@Spectracom ~ $ tracepath -p 123 10.1.2.8
 1: send failed
Resume: pmtu 65535
spadmin@Spectracom ~ $
```

What is the **"Reach"** value for **"nytime"** (its row) in this `ntpq -q` response? Note it should be **"377"** if it can get receive good NTP packets from nytime (such as what is being reported in the second row of the screenshot above). If it's a **"0"**, this SecureSync is not getting any NTP packets from nytime, or the NTP packets are indicating nytime is not in sync/Stratum1

The response to this command should list nytime's IP address/DNS host name in the first column. First try pinging this value (exactly as shown in the `ntpq -p` response) from the command prompt to ensure there is a response from nytime

to this SecureSync.

Then at its command prompt, type the following: `traceroute -p 123 time.spectracomcorp.com` As shown below, verify the last value is **63.138.60.57** (note this IP address may vary) followed by **"reached"** at the end of the line:

```
Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
1?: [LOCALHOST] pmtu 1500
1: 10.2.1.1 2.353ms
1: 10.2.1.1 2.239ms
2: 74.112.39.70 2.165ms reached
Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

Repeat this same command above, but replace "time.spectracomcorp.com" (at the end of the command) with the exact IP/hostname for "nytime" (As reported in the ntpq -p response). The last value in this response should be the IP address of "nytime" (instead of 74.112.39.70) followed by **"reached"** at the end of the line (assuming nytime is routable from dentime and that port 123 is open all the way through).

### ability to run traceroute with the TCP option

- added this capability in v5.8.3 (and above)

#### per the version 5.8.3 Release Notes

"Created opportunity for customers with admin privileges to run traceroute with the TCP option"

B)

### C) Tracepath (for some versions of software prior to 5.8.1ish)

**Note:** Can specify a particular port (such as port 123) to confirm its open all the way through (more info on this further below) Example `tracepath -p 123 time.spectracomcorp.com` (IP address of 63.138.60.57)

**Function:** From tracepath man page: "It traces path to *destination* discovering MTU along this path. It uses UDP port *port* or some random port. It is similar to **traceroute**, only does not require superuser privileges and has no fancy options."

- **IPv4:** Type **"tracepath"** followed by the destination address.
- **IPv6:** Type **"tracepath6"** followed by the destination address.

```
spadmin@Spectracom ~ $ tracepath 10.2.1.1
1?: [LOCALHOST] pmtu 1500
1: 10.2.1.1 2.164ms reached
1: 10.2.1.1 2.104ms reached
Resume: pmtu 1500 hops 1 back 64
```

Note: it appears tracepath may no longer work in at least 5.8.2 (if not earlier, also)

### tracepath using a specified port number (such as port 123)

- Switch "-p" allows a desired port number to be specified

**tracepath -p 123 time.spectracomcorp.com** As shown below, verify the last value is **74.112.39.70** followed by **"reached"** at the end of the line:

```
Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
1?: [LOCALHOST] pmtu 1500
1: 10.2.1.1 2.353ms
1: 10.2.1.1 2.239ms
2: 74.112.39.70 2.165ms reached
Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

**Example of a destination address not being available via port 123 (“send failed” to a bad address)**

```
spadmin@Spectracom ~ $ tracepath -p 123 10.1.2.8
1: send failed
Resume: pmtu 65535
spadmin@Spectracom ~ $
```

What is the “**Reach**” value for “nytime” (its row) in this ntpq -q response? Note it should be “377” if it can get receive good NTP packets from nytime (such as what is being reported in the second row of the screenshot above). If it’s a “0”, this SecureSync is not getting any NTP packets from nytime, or the NTP packets are indicating nytime is not in sync/Stratum1

The response to this command should list nytime’s IP address/DNS host name in the first column. First try pinging this value (exactly as shown in the ntpq -p response) from the command prompt to ensure there is a response from nytime to this SecureSync.

Then at its command prompt, type the following: `tracepath -p 123 time.spectracomcorp.com` As shown below, verify the last value is **63.138.60.57** (note this IP address may vary) followed by “**reached**” at the end of the line:

```
Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
1?: [LOCALHOST] pmtu 1500
1: 10.2.1.1 2.353ms
1: 10.2.1.1 2.239ms
2: 74.112.39.70 2.165ms reached
Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

Repeat this same command above, but replace “time.spectracomcorp.com” (at the end of the command) with the exact IP/hostname for “nytime” (As reported in the ntpq -p response). The last value in this response should be the IP address of “nytime” (instead of 74.112.39.70) followed by “**reached**” at the end of the line (assuming nytime is routable from dentime and that port 123 is open all the way through).

---

## Dig: (Domain Information Groper)

Note (24 Jan KW) Appears dig may have removed (or disabled for spadmin)

- type “**dig**” followed by address

**Function:** a flexible tool for interrogating **DNS name servers**. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

```
1 10.2.100.35 <10.2.100.35> 1.275 ms 0.326 ms 0.268 ms
spadmin@Spectracom ~1$ dig 10.2.100.35

<<>> DiG 9.4.1-P1 <<>> 10.2.100.35
; global options: printcmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 27049
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

; QUESTION SECTION:
10.2.100.35.                IN      A

; AUTHORITY SECTION:
n-grs.com. 2012042001 1800 900 604800 86400      IN      SOA      a.root-servers.net. nstld.verisi

; Query time: 120 msec
; SERVER: 10.1.1.30#53<10.1.1.30>
; WHEN: Fri Apr 20 18:29:31 2012
; MSG SIZE rcvd: 104

spadmin@Spectracom ~1$
```

## netstat and ss commands (portscan to see which ports are open)

- Refer to “netstat” section in the Custserviceassist doc: ..\CustomerServiceAssistance.pdf
- Function: Shows network connections, routing tables, network status

<https://www.tecmint.com/find-open-ports-in-linux/>

To list all open ports or currently running ports including TCP and UDP in Linux, we will use **netstat**, is a powerful tool for monitoring network connections and statistics.

```
List All Network Ports Using Netstat Command

$ netstat -ltnu
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:22              :::*                     LISTEN
tcp    0      0 0.0.0.0:80              :::*                     LISTEN
tcp    0      0 0.0.0.0:25              :::*                     LISTEN
udp    0      0 0.0.0.0:68              0.0.0.0:*               *
```

Where,

- **-l** - prints only listening sockets
- **-n** - shows port number
- **-t** - enables listing of tcp ports
- **-u** - enables listing of udp ports

- just type “**netstat**”, or can optionally add various combinations of switches (list together)
- For more parameters and info, refer to: <http://en.wikipedia.org/wiki/Netstat> and <https://www.tecmint.com/20-netstat-commands-for-linux-network-management/>

## netstat -ltnu / ss -ltnu commands

- Refer to <https://www.tecmint.com/find-open-ports-in-linux/>
- spadmin account has rights to perform this command

**Note:** Can also search for a particular port (such as port 8080 for the classic web browser interface, as an example) to see if this port is enabled: **netstat -ltnu | grep 8080**<enter>. A null response (as shown below) indicates that port is closed.

```
spadmin@spectracom /etc $ netstat -ltnu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 127.0.0.1:705           0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:22              :::*                     LISTEN
tcp    0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
udp    0      0 0.0.0.0:68              0.0.0.0:*               *
udp    0      0 10.2.192.227:123        0.0.0.0:*               *
udp    0      0 127.0.0.1:123           0.0.0.0:*               *
udp    0      0 0.0.0.0:123            0.0.0.0:*               *
udp    0      0 0.0.0.0:161            0.0.0.0:*               *
udp6   0      0 fe80::2d0:c9ff:fec9:123 :::*                      *
udp6   0      0 :::123                  :::*                      *
udp6   0      0 :::123                  :::*                      *
udp6   0      0 :::161                  :::*                      *
spadmin@spectracom /etc $ netstat -ltnu | grep 8080
spadmin@spectracom /etc $
```

You can also use ss command, a well known useful utility for examining sockets in a Linux system. Run the command below to list all your open TCP and UCP ports:

```
List All Network Ports Using ss Command

$ ss -ltnu
Netid State  Recv-Q Send-Q Local Address:Port      Peer Address:Port
udp    UNCONN 0      0 *:*68                  *:*
tcp    LISTEN 0      128  :::22                  :::*
tcp    LISTEN 0      128  *:*22                  *:*
tcp    LISTEN 0      50   *:*3306                 *:*
tcp    LISTEN 0      128  :::80                  :::*
tcp    LISTEN 0      100  :::25                  :::*
tcp    LISTEN 0      100  *:*25                  *:*
```

Make it a point to read through the man pages of the commands above for more usage information.

---

## Loopback interface/logical interface

- Refer to SR 6212 in SAP
- Refer to sites such as:  
[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/interface/configuration/guide/finter\\_c/icflogin.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/interface/configuration/guide/finter_c/icflogin.html)

**Email from Paul Myers (8 Aug 16)** They are thinking we are like a CISCO router.

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/interface/configuration/guide/finter\\_c/icflogin.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/interface/configuration/guide/finter_c/icflogin.html)

I don't think I have an answer at this time as we did not support this. I don't know if we have an alternative interpretation of how to relate what we do to this. Are they talking about NTP interface only?

**Loopback interface:** a software-only, virtual interface that is always up and and allows BGP sessions to stay up, even if the outbound interface is down,.

*From the link above(referring to a Cisco Router):*

You can specify a software-only interface called a loopback interface to emulate an interface. Loopback interfaces are supported on all platforms. A loopback interface is a virtual interface that is always up and allows Border Gateway Protocol (BGP) and remote source-route bridging (RSRB) sessions to stay up even if the outbound interface is down.

You can use the loopback interface as the termination address for BGP sessions, for RSRB connections, or to establish a Telnet session from the device's console to its auxiliary port when all other interfaces are down. You can also use a loopback interface to configure IPX-PPP on asynchronous interfaces. To do so, you must associate an asynchronous interface with a loopback interface configured to run IPX. In applications in which other routers or access servers attempt to reach this loopback interface, you should configure a routing protocol to distribute the subnet assigned to the loopback address.

Packets routed to the loopback interface are rerouted back to the router or access server and processed locally. IP packets routed out the loopback interface but not destined to the loopback interface are dropped. This means that the loopback interface serves as the Null 0 interface also.

---

## Samba software

**Samba:** "Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients." Samba is freely available, unlike other SMB/CIFS implementations, and allows for interoperability between Linux/Unix servers and Windows-based clients.

Q- I asked Paul M if SecureSyncs/9400s use Samba

**A Reply from Paul (5/30/17) regarding SecureSyncs.9400s (as of at least v5.7.0).** No the shipping product does NOT use samba. We can use it for development on the VMs, but shipping SecureSync's do NOT use this.



---

## Nessus Credentialed scans/vulnerability scans

### Credentialed vulnerability scans/elevated Credentialed scans

- Customers can perform a credentialed scan using the spadmin account
- Elevated credentialed scans are “deep OS” vulnerability scans requiring root-level login access
  - As of at least June 2023, we do not provide this level access to anyone outside of Engineering.
  - So, with each software update release, we internally perform an elevate credentialed scan and post the results of the scan in the associated Software release ECO (in SAP)

Q And our customer need scan every month the Server for policies. If it's possible make a special user for that or what is your recommendation.

**A Keith's response (27 Sept 2019)** For security reasons, we do not provide root level access to the SecureSync to anyone outside of the Orolia Engineering team. However, I will forward your request over to the SecureSync's Product Manager for his consideration!!!

### 1200 SecureSyncs lock-up during Nessus scans

- Refer to Salesforce Case 301007
- Appears to be due to the units having 1<sup>st</sup> gen ETX module (32 bit) installed instead of 2<sup>nd</sup> generation ETX module (64 bit) installed. 2<sup>nd</sup> gen ETX module is more powerful.

## \*\*\*\*user accounts and passwords (root/spadmin/spfactory/spui etc )

- Refer to online SecureSync user guide for more info:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/UserAccounts.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/UserAccounts.htm)

(Internal use only) Shadow file: Viewing all accounts via the CLI interface:

1. spectracom/etc
2. type: **getent shadow**.
3. Scroll down to the bottom of the response.

**Note:** Refer to Shadow in all products for deciphering this response.

```
spfactory@Spectracom/etc
spfactory@Spectracom /etc $ getent shadow
halt:*:9797:0:0:0:
operator:*:9797:0:0:0:
shutdown:*:9797:0:0:0:
sync:*:9797:0:0:0:
bin:*:9797:0:0:0:
daemon:*:9797:0:0:0:
adm:*:9797:0:0:0:
lp:*:9797:0:0:0:
news:*:9797:0:0:0:
uucp:*:9797:0:0:0:
nobody:*:9797:0:0:0:
man!:15818:0:0:0:
sshd!:15818:0:0:0:
cron!:15885:0:0:0:
dhcp!:15885:0:0:0:
ftp!:15885:0:0:0:
ntp!:15885:0:0:0:
stunnel!:15885:0:0:0:
ldap!:15885:0:0:0:
apache!:15885:0:0:0:
nullmail!:15885:0:0:0:
feron!:15885:0:0:0:
mysql!:15885:0:0:0:
spui!:16176:0:99999:7:0:
spadmin:$1$a0P9NVVT$8VOU8EP7awhQs63mq9vRT.:16176:0:99999:7:0:
root:$1$z0.7Xhnt$yjdYK51.IVAVVLI.hIbpK.:16176:0:0:0:
spfactory:$1$T6ODD0uk$I9sr$KpaYEuQe0euhkabh.:16176:0:99999:7:0:
oleg:$1$gwwmFVb$A0jilsgsfZH4RWAatFiR0/:16189:0:99999:7:0:
spfactory@Spectracom /etc $
```

CLI command **cat /etc/passwd | grep -v nologin | grep /bin/bash**

root:x:0:0:root:/root:/bin/bash **This entry is for the root user, Linux.**

spfactory:x:1000:110:./root:/bin/bash default **This entry is for factory default login for Web U/I, CLI, and configuration.**

spui:x:1001:0:./home/spectracom:/bin/bash? **This entry is for the user of the Web U/I**

spadmin:x:1002:111:./home/spectracom:/bin/bash default **This entry is the factory default login for web U/I and CLI through serial or SSH terminal**

**Statement from Dave Sohn (Can be sent to customers) 20 Dec 2017**

To Whom It May Concern;

The Spectracom SecureSync provides remote access through only the spadmin and spfactory default accounts. The spfactory account password is only available to Spectracom employees for production and support use. However, the spfactory login can be disabled by the user, if desired.

All other accounts displayed in Linux such as root and spui etc are not accessible for remote access.

Summary table for Accounts (created by a customer and approved by Dave Sohn on 28 Mar 17)

| <u>Account</u>           | <u>Roles</u>                                          | <u>Login method</u>                                                                  | <u>Account and Password owner</u> | <u>Can it be removed and what is the impact</u> | <u>Password can be reset / kept by user</u> |
|--------------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------|---------------------------------------------|
| <b>spadmin</b>           | Admin account                                         | Access via Ethernet (browser/CLI) or RS-232 (front panel Serial port)                | Machine owner                     | It cannot be removed                            | Yes / Yes                                   |
| <b>Root group member</b> |                                                       |                                                                                      |                                   |                                                 |                                             |
| <b>spfactory</b>         | Factory account for factory engineer logon at factory | Access via Ethernet, RS-232                                                          | Manufacturer only                 | It can be removed. No impact.                   | No/No                                       |
| <b>spui</b>              | Web UI                                                | No Access                                                                            | Manufacturer only                 | It cannot be removed                            | No/No                                       |
| <b>root</b>              | OS super-user account                                 | Cannot direct logon access. Must fist login as either spadmin or spfactory then "su" | Manufacturer only                 | It cannot be removed                            | No/No                                       |

**Note:** Details for each account are below

#### D) spadmin account/password

- unlike spfactory account, spadmin account cannot be deleted/removed

**Username:** spadmin

**Password:** admin123

#### Desire to optionally delete/remove the spadmin account from the SecureSync

- Refer to Case 217448 (Dec 2019, related to update version 5.8.6)

Q For Security reason, we would like to delete the "spadmin" login after we created our own login in admin group. Currently, the GPS doesn't give us the option to delete the "spadmin" login after I created our own "admin" login. Is there a way to delete the "spadmin" login?

**A Keith's response (after discussing this with Dave Sohn, 5 Dec 2019):** I just spoke to the SecureSync Senior Product Manager about this question, since I don't recall anyone previously asking about the desire to remove the spadmin account.

Your understanding of the SecureSync not providing the ability to remove/delete the spadmin account is correct. This desired capability isn't available. The Product Manager mentioned that our Engineering team had previously considered being able to optionally remove it (and had even started implementing code changes to support it) but due to concerns of the unit potentially getting into a state where there were no available accounts with admin rights, this function change was stopped. This potential condition of ending up with no admin accounts would then prevent any changes from being implemented.

Since this account cannot be deleted, my suggestion is to assign it an "ultra complex" password.

#### E) spfactory account/password

**Username:** spfactory

**Password:** (not provided here for security reasons)

**Per Dave Sohn (20 Dec 17)** The spfactory account password is only available to Spectracom employees for production and support use. However, the spfactory login can be disabled by the user, if desired.

**Function:** The spfactory account provides our Engineers with the ability to able to remotely connect and have root access to the server, if it was necessary for some reason (root privilege is only available by first logging into the spfactory account). The spfactory account can be safely removed with no

detrimental effects (We just will be no longer able to remote in with root permissions).

### Deleting the spfactory account

- This account provides our Engineers with the ability to able to remotely connect and have root access
- Once this account has been deleted, it can't be re-enabled, unless the unit is restored to factory defaults (not just cleaned or updating the software to a newer version. We can no longer remote in with root permissions.
- There are no other detrimental effects of deleting the spfactory account.

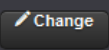
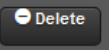
The spfactory account provides our Engineers with the ability to able to remotely connect and have root access to the server, if it was necessary for some reason (root privilege is only available by first logging into the spfactory account). The spfactory account can be safely removed with no detrimental effects (We just will be no longer able to remote in with root permissions).

However, once the spfactory account has been deleted, it can't be re-enabled, unless the unit is "restored to factory defaults" (not just "cleaned" or the software updated to a newer version).

### 1. Using the newer web browser (versions 5.1.2 and above) to delete the spfactory account

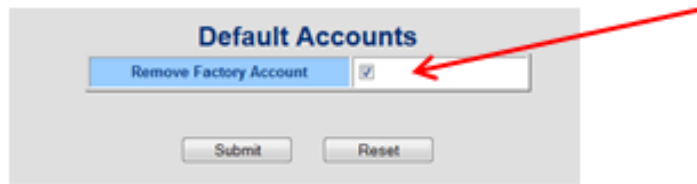
Note: Once the spfactory account has been deleted, it can't be re-enabled, unless the unit is "restored to factory defaults" (not just "cleaned" or the software updated to a newer version).

- 1) Login as spadmin or other custom account in the Admin group (custom accounts in the User group don't have permissions to delete the spfactory account)
- 2) Navigate to the **Management** -> **Authentication** page of the browser
- 3) Under "**Users**", press the **Delete** button next to spfactory.

| Username  | Group   | Notes |                                                                                       |
|-----------|---------|-------|---------------------------------------------------------------------------------------|
| spadmin   | admin   |       |  |
| spfactory | factory |       |  |

### 2. Using the Classic interface browser to delete the spfactory account

- 1) Login as spadmin or other custom account in the Admin group (custom accounts in the User group don't have permissions to delete the spfactory account)
- 2) Navigate to the **Tools** -> **Users** page of the browser, **Security** tab
- 3) At the bottom of this tab (under "**Default Accounts**"), select the checkbox next to "Remove Factory Account" and press Submit.



### F) spui account

- Also refer to info/emails in:  
../EQUIPMENT/SPECTRACOM%20EQUIPMENT/SecureSync/Accounts%20(root%20and%20spui)
- account used internally only for the web browser
- must be logged into root to access spui (can't log directly into spui)



## G) Root account / Root password (OS super-user account)/ pam\_securetty.so file

➤ Also refer to info/emails in:

[././EQUIPMENT/SPECTRACOM%20EQUIPMENT/SecureSync/Accounts%20\(root%20and%20spui\)](mailto:././EQUIPMENT/SPECTRACOM%20EQUIPMENT/SecureSync/Accounts%20(root%20and%20spui))

### Logging in as root

#### Remote access to the root account is not available/blocked

- **v5.8.1 and below:** direct connect to root account via serial cable only (see note belowm indicating this will be changing in 5.8.2 and above)
- **v5.8.2 and above Note email from Ron Dries (16 Aug 2018) before 5.8.2 was released** The front panel RS-232 serial port does currently allow root login (v5.8.1 and below). However, we intend on changing this front panel functionality in the next SecureSync software update (version 5.8.2) , so that root login won't be available with a direct serial connection, either

**Per Dave Sohn (20 Dec 17)** "...All other accounts displayed in Linux, such as root and spui, etc, are not accessible for remote access."

Q Does the root account have interactive logon privileges?

**A Keith's response:** NO. Root is for factory use only and you **have to attach directly to the processor board inside the chassis to be able to login as root** (cannot connect to root via Ethernet connection).

Q If so, by what mechanism do I change the root password?

**A Keith's response:** You cannot delete the root account, but it is not useable unless you gain physical access to physical connections inside of the SecureSync. You cannot change its password. However, you can delete the **spfactory** user from the **Management->Authentication** page of the browser to meet this goal. We don't login as root, but login as spfactory and can then use sudo to do 'root things'.

You must delete/remove the spfactory account to meet this requirement.

#### Q Why we do not disclose the root password

**A Email from Paul Myers to Wade Sober (8 July 2013)** We do not give out the Root password because we do not want configuration changes made to the product, as they can destroy the software stability or installation.

### Note about root account

**Much earlier Email from Mike Sander:**The only way to get at the "root" account is log-in as another user, then switch to root. There is no way to log on directly as "root", not through the serial port and certainly not remotely.

Once the user changes the spadmin password, there is no way for anyone to use the root password without also knowing a password created by the customer.

Our position is that root is not an account, in the sense that it does not provide access to the system.

#### Keith's response to customer

To begin, root is not an available login account, because there is no way to directly login to the appliance with a root account. The highest login account is the default "spadmin" account. The root account is barred from being a login account on all ports, including the Ethernet interface and the front panel interfaces (keypad and SERIAL port).

Root can only be accessed through another login account, such as the default "spadmin" account or a user account that has been created. Once a user changes the default spadmin password (as is highly recommended, since the spadmin password is a published value), there is no way to access root without knowing the new spadmin account passwords (or one of the user account passwords), even if someone was to know what the root password happens to be.

**Another Email Keith sent:** Though it's not possible to directly deactivate the root account directly, it is possible to remove access to it. Access to the root account is only available via either the factory default "spfactory" account or another user account (Access to root is only available after logging into a user account and then switching to root). The spfactory account can be removed, if desired, thereby removing access to the root account via the spfactory account. Once the spfactory account has been removed, and the spadmin account password has been changed from the default value (as is highly recommended, since the spadmin password is a published value), access to root is no longer available.

The “spfactory” account can be deleted as desired, thereby removing all access to the root account from that point forward (unless a restore to factory defaults is performed using the software update process- not just by performing a standard “clean” of the configurations).

### To remove the default spfactory account (inhibiting access to the root account)

- Refer to the “spfactory account” info in the next section below.

### Must be logged into the root account first, to have access to the spui account (cannot log directly into spui)

**Note:** details/email exchanges below were with Ron Dries for WAPA (~July/Aug 2018)

- In the PAM config files, we use **pam\_securetty.so** to ensure that the root account cannot be logged into. There is a config file in SecureSyncs called **securetty** (as in “secure tty”) which lists the terminals that root is allowed to login to.
- Q As mentioned before, when we look at the output of the local “passwd” file indicates that a Shell is available to them so that makes it appear as though we can login into them. For compliance purposes, we need to be able to provide evidence. Since we cannot change the password on root and spui, we need to be able to either prove that they cannot be logged into or show vendor documentation that the passwords were generated pseudo-randomly and are thereby unique to the device.

We need your assistance to find a command or setting in a local file to prove they cannot be logged into, or some documentation asserting that the passwords are random and unique.

**A Reply from Keith (based on info from Ron)** In the PAM config files, we use **pam\_securetty.so** to ensure that the root account cannot be logged into. There is a config file in SecureSyncs called **securetty** (as in “secure tty”) which lists the terminals that root is allowed to login to.

In the next SecureSync software version upgrade (**note from Keith- Should be in 5.8.2**), this will be updated to also not allow root login from the front panel serial port.

Here is an example of the PAM login config file, with the line that uses this config file highlighted:

```
cat /etc/pam.d/login
auth include /etc/tacacs_pam.conf
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
account required pam_securetty.so
account include /etc/tacacs_pam.conf
account required pam_tally.so
account sufficient pam_unix.so
account required pam_deny.sols
session include /etc/tacacs_pam.conf
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session required pam_unix.so
password required pam_unix.so shadow md5
```

- Q What about the spui account? How do we prove that it can't login. Does the securetty clearly show that root can't login? What about spui? I couldn't find in ssh\_config where this is related. If we configure in the /etc/security/access.conf to deny root and spui tty access would that work or is it ignored by the system?

**A (email from Ron)** In the /etc/shadow file for spui there is an “!” for spui.

The “!” point means the password is locked and login with a Unix password is disabled.

The root user is the only user that is able to get access to spui.

An empty securetty file will disable root login for any console device. This will be added in the next release.

The ssh\_config file has “PermitRootLogin no”.

Q (from Case I couldn't find the file securetty. I found the library pam\_securetty.so but it's an executable and I can't see anything in it. I also found that there is an access.conf file in /etc/security which looks like it can limit login access but it is not configured.

I need a file I can look into which indicates root and spui can't login.

---

---

### **Protection/encryption of local account passwords**

- Refer to (in this document): [\\*\\*\\*/etc/shadow \(Linux password file\)](#)
-



## User accounts / Permissions

### Creating new accounts/Editing accounts

#### As of at least Archive version 4.8.9:

- SecureSync's user accounts can only be managed (editing user names, changing passwords, etc) via the web browser (HTTP/HTTPS)
- User accounts cannot be created or edited via CLI commands using telnet or SSH.

---

### viewing user accounts/CLI command to list all users

#### **getent passwd**<enter>

- created user accounts and Passwords are stored/viewed in **"/etc/shadow"** (customers cannot view with spadmin. Must be logged in as **spfactory** to view the contents of this file)

**Per Ron Dries (21 April 2020)** For a command line way to list users, including LDAP users, issue the following command:  
**getent passwd**<enter>

---

### Rules for usernames (versions 5.1.2 and above, when using the newer browser)

- **Length:** Can be between 3 and 32 characters long.
  - **Must start** with a lower-case letter.
  - All letters must be lower-case.
  - **Accepts:** all letters, numbers, underscores and dashes. It **does not** accept special characters such as the following characters  **! @ # \$ % ^ & \* ( )**
- MAX Number of accounts that can be created: Per Ron Dries (21 Oct 2014) he is not aware of any established limit on the number of user accounts that can be created. There should be no limit.
    - **Newer browser (versions 5.1.2 and above)** Accounts and passwords are managed in the **Management -> Authentication** page of the browser. Click on the "+" sign in the upper-right corner to create new user accounts.
    - **Classic Interface** Accounts and passwords are managed in the **Tools -> Users** page of the browser

*Users* can be assigned to be in either the user group or the admin group. Users in the admin group can't make configurations changes. Configuration changes can only be made via the Admin account or a user account that is in the Admin group.

The **Tools -> Users** page allows password management (in order to edit User accounts, have to be logged in as either Admin or a user account that is configured to be in the admin).

### Permissions

- Group Rights/privileges are exactly the same for both SSH and web browser login
  - Note:** Information below is based on version 5.1.2 (future versions may change this info)
  - Note:** Red text below indicates items that are different for the group as compared to the spadmin account

### spadmin account

No limitations  
Can manage passwords/user accounts

**admin group**

No limitations  
Same as spadmin account

**user group**

I'll start by saying the privileges for user and admin groups are exactly the same whether logging in via the web browser or connecting via SSH.

The following is the information for the new web browser with version 5.1.2 software installed. The easiest way to see the differences is to compare the web browser menus for an admin and a user side-by-side. You will then be able to notice what capabilities are not available to those that login with SSH or the browser as a member of the user group.

---

**1. Tools menu**



**Logs:** Limited logs can be viewed by user (only the listed logs can be viewed)

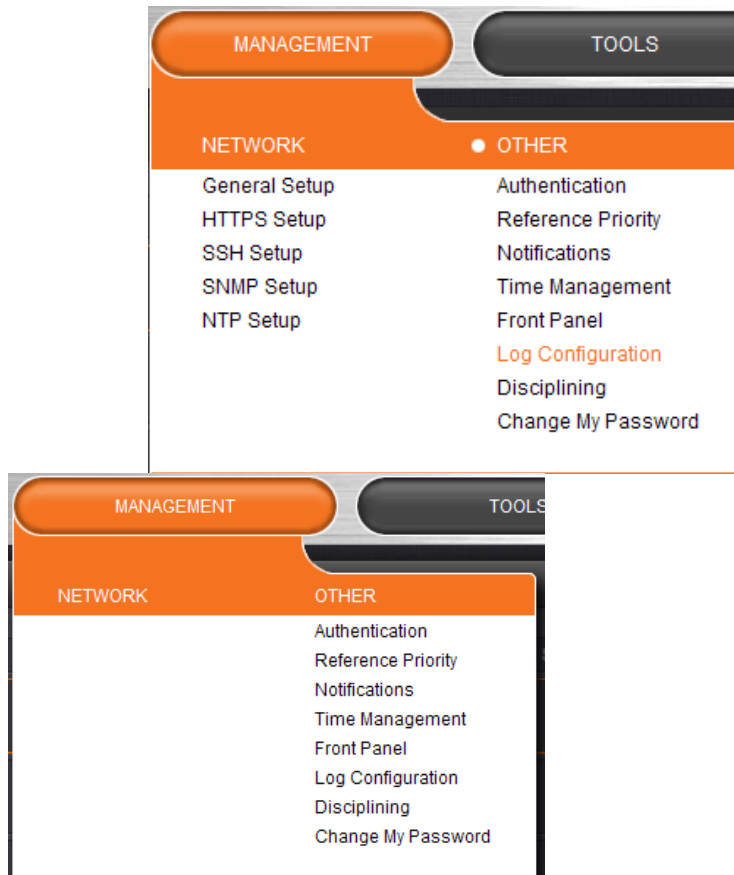
**Upgrade/Backup:** User cannot access this page (Goes to the Home page). Can't perform any updates.

**Reboot/Halt:** User cannot access this page. Can't reboot/shutdown/halt.

**2. Management menu**

**With admin rights**

**with only user rights**

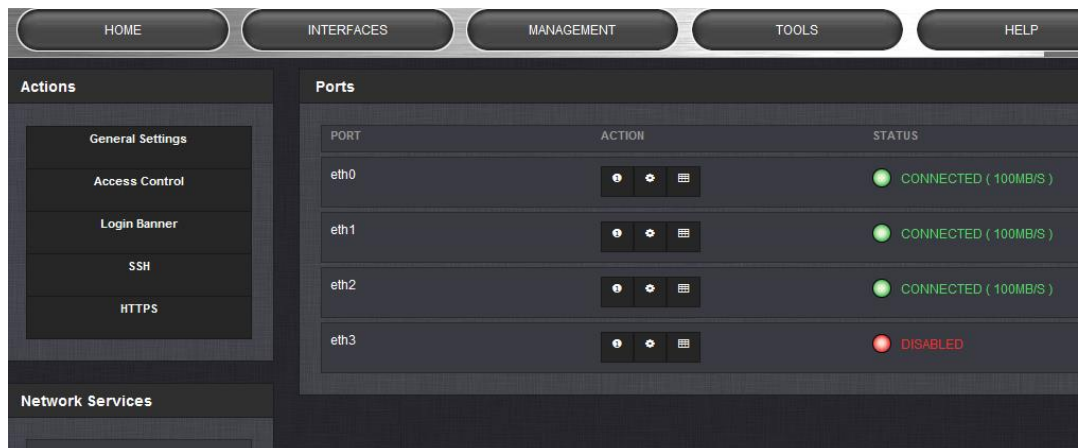


**Network:** Users cannot modify any of the network-related configurations (if they click on “Network”), they can only view the **Tools** -> **Network** page. But they can’t make any modifications to this page. They cannot access HTTPS, SSH, SNMP or NTP pages (cannot view or change current settings).

As shown below, when logged in as user and “Network is selected, the “Actions” buttons (for General Settings, Access Control, login banner, SSH and HTTPS) normally located on the left-side of the screen is not available. Also, when logged in as a user, the only one of the three normally available boxes for the ports is the status box (users can’t make changes to the network settings or disable Ethernet ports).

#### admin account:

These selections are only available as spadmin



#### User account

HOME INTERFACES MANAGEMENT TOOLS HELP

**Network Services**

- Daytime Protocol  OFF
- Time Protocol  OFF
- Telnet  ON
- FTP  ON
- SSH  ON
- HTTP  ON
- HTTPS  ON

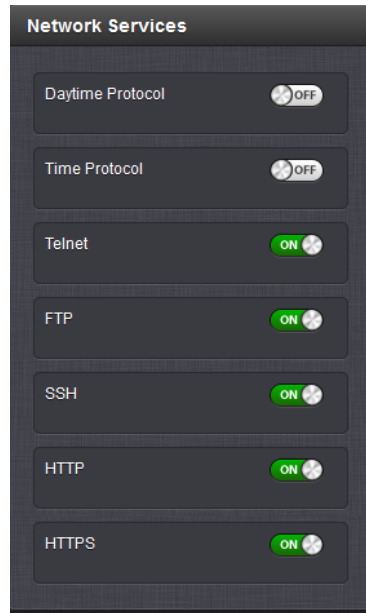
**Ports**

| PORT | ACTION                   | STATUS                |
|------|--------------------------|-----------------------|
| eth0 | <input type="checkbox"/> | CONNECTED ( 100MB/S ) |
| eth1 | <input type="checkbox"/> | CONNECTED ( 100MB/S ) |
| eth2 | <input type="checkbox"/> | CONNECTED ( 100MB/S ) |
| eth3 | <input type="checkbox"/> | DISABLED              |

Only the Status window selection is available as a user.

**Network Services (such as telnet, FTP, SSH and HTTP/HTTPS):** Can move the switches, but they won't do anything. So a user cannot enable or disable any Services. Browser will report "Setting FTP Failed" if a switch is moved.

"Network Services" Switches do not allow a "user" to be able to enable or disable any Services (must be an admin to enable/disable)



**Authentication:** Users can access this page but can only change their own password. Users cannot create any new accounts and can't modify any accounts, other than changing their own password.

**Reference Priority:** Users can access this page and modify settings.

**Notifications:** Users can access this page and modify settings.

**Time Management:** Users can access this page and modify settings.

**Front panel:** Users can access this page and modify settings.

**Log Configuration:** Users can access this page and modify settings.

**Disciplining:** Users can access this page and modify settings.

**Change my password:** Users can access this page and change only their password.

## Interfaces menu

**Note:** No differences in privileges for this menu and all items listed. User and admin accounts can view and modify all settings in these pages (can view/edit GPS receiver, outputs and Option Cards)

### admin

| INTERFACES     |                |                |
|----------------|----------------|----------------|
| INTERFACES     | MANAGEMENT     | TOOL           |
| REFERENCES     | OUTPUTS        | OPTION CARDS   |
| GNSS Reference | IRIG Output    | Main           |
| GNSS 0         | IRIG Output 0  | GNSS 0         |
|                | 10 MHz Output  | PPS Output 0   |
|                | 10 MHz 0       | 10 MHz 0       |
|                | ASCII Output   | NENA           |
|                | ASCII Output 0 | IRIG Output 0  |
|                | ASCII Output 1 | ASCII Output 0 |
|                | PPS Output     | ASCII Output 1 |
|                | PPS Output 0   | Alarm Output 0 |
|                | Alarm Output   | Alarm Output 1 |
|                | Alarm Output 0 | Gb Ethernet    |
|                | Alarm Output 1 | Unknown 0      |

### user

| INTERFACES     |                |                |
|----------------|----------------|----------------|
| INTERFACES     | MANAGEMENT     | TOOL           |
| REFERENCES     | OUTPUTS        | OPTION CARDS   |
| GNSS Reference | IRIG Output    | Main           |
| GNSS 0         | IRIG Output 0  | GNSS 0         |
|                | 10 MHz Output  | PPS Output 0   |
|                | 10 MHz 0       | 10 MHz 0       |
|                | ASCII Output   | NENA           |
|                | ASCII Output 0 | IRIG Output 0  |
|                | ASCII Output 1 | ASCII Output 0 |
|                | PPS Output     | ASCII Output 1 |
|                | PPS Output 0   | Alarm Output 0 |
|                | Alarm Output   | Alarm Output 1 |
|                | Alarm Output 0 | Gb Ethernet    |
|                | Alarm Output 1 | Unknown 0      |

## Account Passwords

### \*\*\*\*/etc/shadow file (Linux password file)

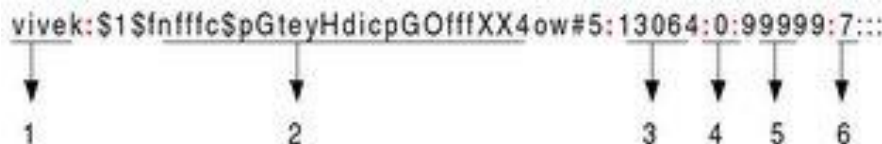
- Refer to: <http://www.cyberciti.biz/faq/understanding-etcshadow-file/>  
<http://searchsecurity.techtarget.com/definition/shadow-password-file>
- Customers (spadmin) do not have permission to view/change this file
  - (“Without root access we can’t view the shadow file The ssh\_config file does not have “PermitRootLogin no” in it).

**/etc/shadow** file stores actual password in encrypted format for user's account with additional properties related to user password i.e. it stores secure user account information. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in [/etc/passwd file](#). Generally, shadow file entry looks as follows (click to enlarge image):

**Per Ron Dries (19 Apr 2019)** The SecureSync uses standard Linux password storage, /etc/shadow file, using a **MD5 hashing algorithm**.

```
Spectracom NetClock 9483 Version 5.1.2
spadmin@Spectracom ~$ /etc/shadow
-bash: /etc/shadow: Permission denied
spadmin@Spectracom ~$ /etc
-bash: /etc: Is a directory
spadmin@Spectracom ~$ /etc
-bash: /etc: Is a directory
spadmin@Spectracom ~$ cd /etc
spadmin@Spectracom /etc$ cat shadow
halt:*:9797:0:0:0:
operator:*:9797:0:0:0:
shutdown:*:9797:0:0:0:
sync:*:9797:0:0:0:
bin:*:9797:0:0:0:
daemon:*:9797:0:0:0:
adm:*:9797:0:0:0:
lp:*:9797:0:0:0:
news:*:9797:0:0:0:
uucp:*:9797:0:0:0:
nobody:*:9797:0:0:0:
man:*:15818:0:0:0:
shd:*:15818:0:0:0:
cron:*:15885:0:0:0:
dhcp:*:15885:0:0:0:
ftp:*:15885:0:0:0:
ntp:*:15885:0:0:0:
stunnel:*:15885:0:0:0:
ldap:*:15885:0:0:0:
apache:*:15885:0:0:0:
nullmail:*:15885:0:0:0:
feron:*:15885:0:0:0:
mysql:*:15885:0:0:0:
spui:*:16097:0:99999:7:0:0:
spadmin:$1$0P9NUIT$8U0U8EP7aahQs63mq9vRT.:16097:0:99999:7:0:0:
adminuser:$1$a2z0Tvtv$e9FYonFLLIc2QXAJFFKpT0:16113:0:99999:7:0:0:
user55:$1$UW1wzITC$N7EMbQCgXsxpLGmRFMxjU0:16113:0:99999:7:0:0:
root:$1$z0_7Xhnt$yjdYK51_IUAUULi_h1bpK.:16097:0:0:0:0:0:0:
spfactory:$1$T6ODD0uk$19sR$KpaVEuQe0euhkabh.:16097:0:99999:7:0:0:
spadmin@Spectracom /etc$
```

### /etc/shadow file fields



- **User name** : It is your login name
- **Password**: It your encrypted password. The password should be minimum 6-8 characters long including special characters/digits
- **Last password change (lastchanged)**: Days since Jan 1, 1970 that password was last changed
- **Minimum**: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
- **Maximum**: The maximum number of days the password is valid (after that user is forced to change his/her password)
- **Warn**: The number of days before password is to expire that user is warned that his/her password must be changed
- **Inactive**: The number of days after password expires that account is disabled
- **Expire**: days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used:

## Protection/encryption of the local account passwords/shadow file

- Encoding/protection of the password file is automatic- no user interaction is required
- we use the standard Linux /etc/shadow file/encryption- we don't change anything
- refer to sites such as <https://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils>

<https://www.oreilly.com/library/view/practical-unix-and/0596003234/ch04s03.html>

[http://web.deu.edu.tr/doc/oreily/networking/puis/ch08\\_06.htm](http://web.deu.edu.tr/doc/oreily/networking/puis/ch08_06.htm)

<https://www.oreilly.com/library/view/practical-unix-and/0596003234/ch04s03.html>

*As the name implies, a shadow password file is a secondary password file that shadows the primary password file. On Solaris and Linux systems, the shadow password is usually stored in the file /etc/shadow and contains the encrypted password and a password expiration date. The /etc/shadow file is protected so that it can be read only by the superuser. Thus, an attacker cannot obtain a copy to use in verifying guesses of passwords.*

[http://web.deu.edu.tr/doc/oreily/networking/puis/ch08\\_06.htm](http://web.deu.edu.tr/doc/oreily/networking/puis/ch08_06.htm)

...UNIX avoids this problem by not keeping actual passwords anywhere on the system. Instead, UNIX stores a value that is generated by using the password to encrypt a block of zero bits with a one-way function called *crypt()*; the result of the calculation is (usually) stored in the file /etc/passwd. When you try to log in, the program /bin/login does not actually decrypt your password. Instead, /bin/login takes the password that you typed, uses it to transform another block of zeros, and compares the newly transformed block with the block stored in the /etc/passwd file. If the two encrypted results match, the system lets you in.

The security of this approach rests upon the strength of the encryption algorithm and the difficulty of guessing the user's password. To date, the *crypt()* algorithm has proven highly resistant to attacks

### two questions from a customer:

- Are local stored credential encrypted? If yes, what type of encryption is used to encrypt local passwords? And how to enable it?
- What type of authentication mechanism used for local authentication? Are there different settings can be configured?

**Answer:** The answers to both questions above is dependant on software version installed (5.5.0 and above/5.4.5 and below)

### A) Software Versions 5.5.0 and above

**Per Paul Myers (6 Mar 17)** The /etc/shadow folder in release 5.5.0 and higher is **permissions 640 and hides user passwords hashes**. Please upgrade to the version 5.5.1.

So access permissions can be expressed as three digits. For example:

|                 | user | group | others |
|-----------------|------|-------|--------|
| chmod 640 file1 | rw-  | r--   | ---    |
| chmod 754 file1 | rwX  | r-X   | r--    |

### B) Software Versions 5.4.5 and below

**Per Ron Dries (24 Feb 16)** As of at least versions 5.4.0 and below, we just use the standard Linux shadow file for storing and protecting passwords. There are some limitations to this encryption mechanism, but a user has to be logged in already in order to access/view the file.

- For more info on the protection of the shadow file, refer to websites such as: <http://searchsecurity.techtarget.com/definition/shadow-password-file>

“The original password is encrypted (or encoded) by using a randomly-generated value or encryption key



between 1 and 4096 and a one-way hashing function to arrive at the encoded password that is actually stored. Note that the stored result is not something that you can enter as a password itself.

- In at least versions 5.8.1 and below, there are no options/capabilities available to change the password protection.
- The shadow file for storing passwords is located: **/etc/shadow**
- The shadow file cannot be viewed by either spadmin or other user accounts (must be logged in as spfactory to view it) (the screenshot below is while logged in as spadmin)

```
cat: shadow-: Permission denied
spadmin@Spectracom /etc $ cat shadow
cat: shadow: Permission denied
spadmin@Spectracom /etc $ cat shadow-
cat: shadow-: Permission denied
spadmin@Spectracom /etc $
```

### **Desire to change the root password and/or spfactory account password**

- The root password and spfactory account password cannot be changed. However, the spfactory account can be deleted, which removes all remote access to the root account.
- Refer to the Account information further above for info on removing the spfactory account to remove access to spfactory and therefore also root.

### **spui account protection**

Q What about the spui account? How do we prove that it can't login. Does the security clearly show that root can't login? What about spui? I couldn't find in ssh\_config where this is related. If we configure in the /etc/security/access.conf to deny root and spui tty access would that work or is it ignored by the system?

A (email from Ron) In the /etc/shadow file for spui there is an "!" for spui.

The "!" point means the password is locked and login with a Unix password is disabled.

## Reset the SPADMIN account password

### Reset the spadmin account password back to default value

#### (v5.9.0 update) Fix to the password not being able to be re-used, for the last 10 passwords

- Per the v5.9.0 Release Notes “Repaired password reuse limitation to cap reuse failures at 10 attempts”

#### A) Via the CLI interface

- If current password is known, **resetpw** CLI command will reset the password back to admin123, even if its been recently changed less than 10 password changes ago (it will override the “remember” of not allowing password re-use before 10 other passwords have been used)

Below is the response to resetpw command (from v5.6.0):

```
spadmin@Spectracom ~ $ resetpw
LDAP_ProcCfgLine: Ignored command: version
LDAP_ProcCfgLine: Ignored command: nss_base_shadow
LDAP_ProcCfgLine: Ignored command: nss_map_objectclass
LDAP_ProcCfgLine: Ignored command: nss_map_objectclass
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_override_attribute_value
LDAP_ProcCfgLine: Ignored command: nss_override_attribute_value
LDAP_ProcCfgLine: Ignored command: referrals
spadmin@Spectracom ~ $ spadmin@Spectracom ~ $ resetpw
```

#### B) Via front panel resetpw command

- The front panel **resetpw** command will reset the password back to admin123, even if its been recently changed less than 10 password changes ago (it will override the “remember” of not allowing password re-use before 10 other passwords have been used).

**Note:** resetpw on front panel also disables LDAP/Radius (versions 5.2.1 and above)

Starting in version 5.2.1 (~~Apr 2015~~) **resetpw also sets LDAP and Radius to “Disabled”** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026 Update- this change was inadvertently left out of the v5.2.1 release. It will need to be added in with the next release (5.3.0?)

#### “Not supported” displayed (v4.8.1 and below only)

**Note:** With Archive Versions 4.8.1 and below installed, a minor bug causes “Not Supported” to be displayed in the LCD, even though the command did reset the password.

Q help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?

**A Keith's response (23 May 17)** Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of 'admin123'.

Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn't change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.

**Note:** Applicable to SecureSync and Model 9483 only (not applicable to 9489)

- When the spadmin account password is known, it can be reset back to factory default via the web browser, front panel keypad or via the front panel SERIAL port.
- If the password is not known, it can be reset back to factory default via the front panel keypad or via the front panel

SERIAL port (web browser won't be accessible without knowing the password).

- The Serial command to reset the password via the Serial port is "resetpw"
  - Front panel keypad admin account password reset is via the **System** -> **Cmd** menus
  - **Versions 5.2.1 (12 May 2015) and above:** resetpw command also disables LDAP and Radius (see additional info below).

**1. (Not applicable to 9489-See further below for 9489) To reset the spadmin password via the front panel keypad**

**Note:** Starting in version 5.2.1 (~~Apr 2015~~) **resetpw also sets LDAP and Radius to "Disabled"** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026 Update- this change was inadvertently left out of the v5.2.1 release. It will need to be added in with the next release (5.3.0?)

When resetpw is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled after performing a resetpw.

**Note:** Applicable to SecureSync and Model 9483 only (not applicable to 9489)

- 1) Press the green checkmark on the front of the unit. This will display the main menus.
- 2) Press the white right arrow keys on the front to highlight "**System**".
- 3) Press the green checkmark.
- 4) Press the white right arrow keys on the front to highlight "**Cmd**".
- 5) Press the green checkmark.
- 6) Then, use the up or down arrow keys to scroll to "**ResetPW**".
- 7) Press the green checkmark.
- 8) Press the green checkmark again to confirm the password reset.

**2. Specific to the Model 9489 (no front panel keypad/LCD available)**

- No keypad available to issue **resetpw**
- Can't login to any CLI interface (including the front panel RS-232 SERIAL port) without knowing the current password.

**To resolve for Model 9489, can:**

- A) Send a new CF card that is programmed with same version of software as the NetClock is running.
  - This method will inherently cause all configs to be restored back to factory default settings. There are other methods listed below which can allow settings to be retained, if desired).
- B) If customer will allow us to remote access (and the spfactory account has not been deleted) login as spfactory, change to root and then type: **passwd spadmin** <enter>. Then type **admin123** to reset it to the factory default value.
  - Unlike replacing the CF card, this method allows current configs to be retained.
- C) Return just the CF card to the factory for password to be reset. Then we return the CF card back to them with the default password.
  - Unlike replacing the CF card, this method allows current configs to be retained.
- D) Return the NetClock to the factory for password to be reset.
  - Unlike replacing the CF card, this method allows current configs to be retained.

---

## Retrieving/Changing user account passwords

### \*\*Retrieving unknown account password

- Passwords can be changed, but can't be retrieved
- Passwords are stored in **"/etc/shadow"**.
- Passwords are "hash" protected (encrypted) when they are created. They can be "viewed" but can't tell what they really are.

### Changing user account passwords

**Note:** Further below are the "rules" for creating/changing usernames and passwords (what's allowed. What's not allowed, etc)

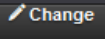
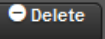
#### C) Via the CLI interface

- The CLI command to change only the spadmin account password (if current password is known) is **passwd**
  - Refer to the CLI section of this document for more info (such as how in at least version 5.6.0 and below, the available 'Password Security' rules don't apply (are bypassed) when the spadmin account password is changed via this cli command): [Available CLI calls \(API calls\)](#)

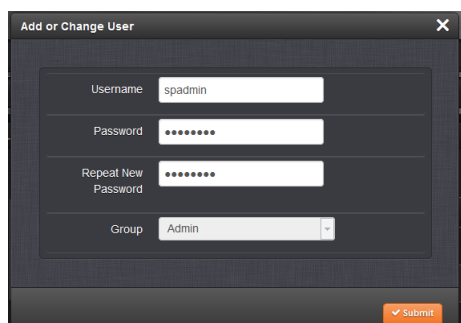
---

#### D) Using the Newer web browser (versions 5.1.2 and above)

- 1) Login as spadmin or other custom account in the Admin group (custom accounts in the user group don't have permissions to change passwords)
- 2) Navigate to the **Management -> Authentication** page of the browser
- 3) Press the **"Change"** button next to the desired account name to change the password

| Username  | Group   | Notes |                                                                                       |
|-----------|---------|-------|---------------------------------------------------------------------------------------|
| spadmin   | admin   |       |  |
| spfactory | factory |       |  |

- 4) This will open a pop-up window. Enter the desired new password and press Submit.



---

#### E) Using the REST API interface (for scripting)

Q Can we change passwords using API? If so, can you please show me how to do it?

A email from Dave Lorah (25 Oct 2019) We have a REST API call that can edit the password of a specific user.

The REST API endpoint to edit a user is: `/users/edit/{username}.json` where `{username}` is the username that you would like to change the password of.

The body that you send in is as follows:

```
{ "User" : { "password" : "test12345", "username" : "{{useredit}}", "repeat" : "test12345" } }
```

 where `{{useredit}}` is the username to edit and `test12345` is the password that we want to set.

## “Change my password” button (newer black/silver browser only)

- This button is on the left side of the [Management](#) -> [Authentication](#) page of the browser
- Applies only to when logged in locally. An error message (discussed further below) occurs when pressing this button while logged in using remote authentication (such as Radius/LDAP/TACACS)
- The pop-up window which opens allows ability to change only the password for the account that user is currently logged into (such as spadmin)
  - A “404: Not Found” error message (discussed below) may be displayed instead of opening the pop-up window which allows the account password to be changed. This indicates the user is likely logged in using remote authentication instead of logged into an account created in the SecureShnc.

## Displayed Error messages of both 404: Not Found and 404: error displayed after pressing “Change my password” button

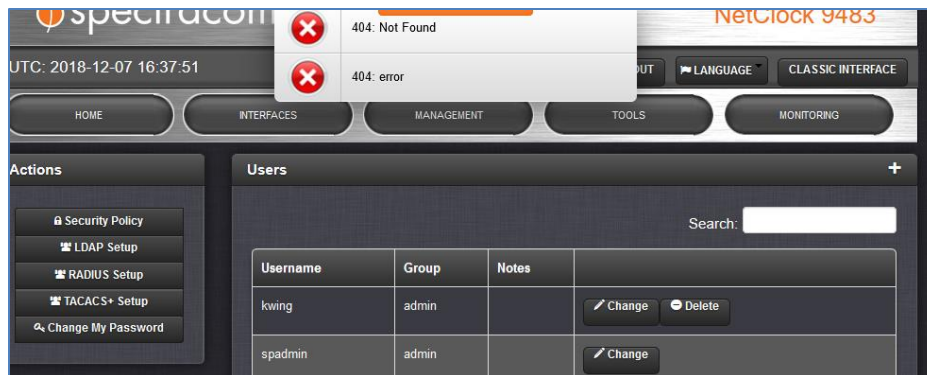


## This Error message is displayed after pressing the “Change my Password” button while currently logged in using remote authentication

**Note** This error message is displayed instead of opening the pop-up window which allows the password to be changed.

### When logged in using remote authentication (Radius, LDAP or TACACS):

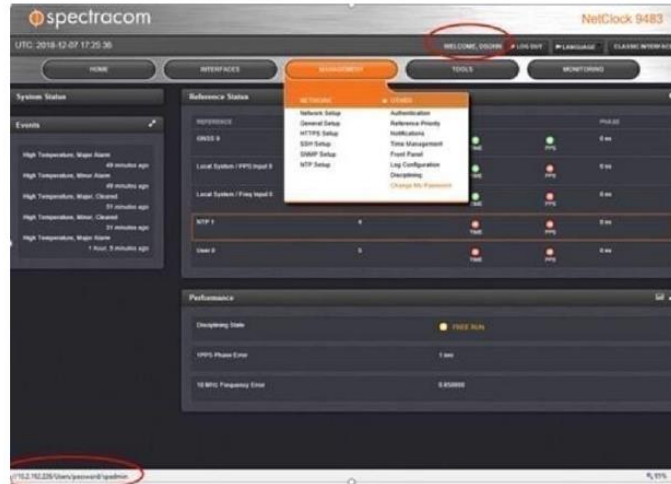
This event is expected, since the account resides in the Remote auth server – not in the SecureSync. Remote authentication passwords need to be managed directly on the remote auth server



**“Caching Issue with Change My Password”: Caching of user account info from the previous login (with at least 5.8.2 and below**

(in at least vesions 5.8.2 and below) after loggingi out of remote auth account and then logging in locally.,while mouse-Hovering over “change my password”. the link at the botton of the page reflected the account previously logged into (instead of the current account)

- Refer to Salesforce case number 179699
- reported by customer, and duplicated here (with firefox/Internet Explorer)



**F) Using the classic interface web browser to change password (v5.8.9 and below)**

1. Login as spadmin or other custom account in the Admin group (custom accounts in the user group don't have permissions to change passwords)
2. Navigate to the **Tools -> Users** page of the browser, “**Manage User Accounts**” tab
3. In the row for the account desired to change the password for (such as spadmin”) type the new password and then re-type the new password.
4. Click “**Update Account**” and then press Submit.

| USER SETUP          |       |                          |                 |                                     |                          |
|---------------------|-------|--------------------------|-----------------|-------------------------------------|--------------------------|
| Create User Account |       | Manage (4) User Accounts |                 | Security                            |                          |
| Username            | Group | Password                 | Retype Password | Update Account                      | Remove Account           |
| spadmin             | admin | ●●●●●●                   | ●●●●●●          | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| quagga              | admin |                          |                 | <input type="checkbox"/>            | <input type="checkbox"/> |
| tcpdump             | admin |                          |                 | <input type="checkbox"/>            | <input type="checkbox"/> |
| winger              | user  |                          |                 | <input type="checkbox"/>            | <input type="checkbox"/> |

## “Password Security” (Available minimum password rules/requirements that can be enforced, if desired)

There are several other minimum password requirements which can be enabled as desired. These include rules such as minimum length of passwords, required use of either capital and/or lower-case letters, numerals, special characters, password expiration (with expiration warning), etc.

These special requirements for creating new passwords going forward or changing existing passwords in the future can be enforced via the “**Security Policy**” (**Management** -> **Authentication** page of the browser. Click on “**Security Policy**” on the left side of the page) as shown below. These minimum password requirements include the following:

### 1. With newer black/charcoal web browser (v5.1.2 and above)

**Note:** Password complexity settings are stored in *pwdcf.conf* file (located in **home/spectracom/config** directory)

*Example below*

```
spadmin@Spectracom ~ $ cd config
spadmin@Spectracom /home/spectracom/config $ cat pwdcf.conf
complx-upper 0
complx-lower 0
complx-number 0
complx-user 0
complx-special 0
age-min 0
age-max 99999
age-warn 7
min-len 8spadmin@Spectracom /home/spectracom/config $
```

- Consists of: password aging, password length, complex passwords and delete the default spfactory account
  - **Software Versions 5.1.2 and above:** in the **Management** -> **Authentication** page of the browser. Click on **Security policy** on the left side of the page
- There are several other minimum password requirements which can be enabled as desired, via “Security Policy” (**Management** -> **Authentication** page of the browser. Click on “**Security Policy**” on the left side of the page) as shown below. These minimum password requirements include the following:



## Customer report: DISA STIG requirement that the spadmin account password never expires

- Refer to SF case 117138

Q The password expiration for the user "spadmin" when we turn on the password policy and are required to change the default shipping password is a CAT 1 DISA STIG failure that will block deployment into the



network. We are using the "spadmin" account as the emergency access account per DISA STIG requirements and the new password should not expire to be compliant. Is there a way to disable this for this account or can we create a true non-expiring emergency account?

**A Reply from Dave L (~23 Aug 17)** I believe all accounts are governed by the same rules and we cannot separate the spadmin from User accounts but I will check and verify this. Please standby while I confirm.

**Created By: Ron Dries (10/17/2017 2:47 PM) | Last Modified By: Ron Dries (10/17/2017 2:47 PM)**

The directory '/var/db/pkg' did not exist in either software versions 5.4.1, or 5.6.0. I am not sure how the Nessus credentialed scan would have passed at 5.6.0 as it should not have been able to find '/var/db/pkg'. There is the potential that the Nessus scan updated, or changed. Further investigations needs to be performed to see if a change in SecureSync software could be causing the issue.

**Dave Sohn (24 Aug 17)** The spadmin account password can be reset to default at any time via the front panel, if necessary. Is that acceptable to resolve the issue?

## B. Account Login Security functions ("Password Security") with the classic interface web browser

- Software Versions 5.0.2 and below: in the **Tools -> Users** page of the browser, **Security** tab

Enhanced logon for Classic web browser versions 5.0.2 and below (Note: this info not applicable to the newer black web browser)

**Note:** enhanced login was started in software version 4.5.0  
(**Tools -> Users** page of the web browser, **Security** tab)

**USER SETUP**

Create User Account | Manage (2) User Accounts | **Security**

**Idle Timeout**

Idle Timeout (minutes) 0

**Password Aging**

Minimum before change (days) 0

Maximum before expiry (days) 99999

Warning before expiry (days) 7

**Password Length**

Minimum Length 8

**Complex Passwords**

Require uppercase Disabled

Require lowercase Disabled

Require number Disabled

Not based on user name Disabled

Require special character Disabled

table special characters include the following: (~@#%\*&\*)\_+ = 00:;<

**Default Accounts**

Remove Factory Account

Submit Reset

- Configurable idle time-outs
- Can either disable or configure how long after no activity before the need to login again note that setting this value to 0 eliminates need to log in again and again).
- Password aging (can enable the ability to either prevent the passwords from being changed, and/or configure them to expire, before or after a configurable amount of time).
- Can remove default factory account
- Password complexity (can enable minimum criteria for new passwords, when they are created)

## From SecureSync manual:

**Require complex passwords:** If enabled, every password must have at least one of each of the following character types:

- Letters (a-z or A-Z)
- Numbers (0-9)
- Special characters ( ~ @ # % ^ & \* ( ) \_ - + = { } [ ] ; < > . | )

The following special characters are NOT allowed: single quote, double quote, dollar sign, comma, backslash, exclamation mark, and apostrophe

Additionally, the username may not be included in the password.

## Complex passwords

When we dug into some of the security standards we found another feature we need - Passwords with at least one of each type: letters, numbers, and special characters.

The feature is configurable on the Security tab of the Tools->Users page.

When complex passwords are enabled, new passwords must include at least one letter, at least one number AND at least one special character ( \_ +=&< etc.

The list of allowed special characters is: ~ @ # % ^ & \* ( ) \_ - + = { } [ ] ; < > . |

**The list of special characters that are not allowed** is: single quote, double quote, dollar sign, comma, backslash, exclamation mark, and apostrophe.

(These characters retain their meaning on a BASH command line, even inside double quotes.)

The software will give you precise feedback if you use one of the not acceptable special characters.

Adam –We already had a feature that passwords can't contain the user name. It used to be always on, but I changed that to be configurable with the same "complex passwords" switch. So if customers don't enable complex passwords, the password for user "mike" can be "mike1234".

Complex passwords will be disabled by default.

## Hard-coded in software (not configurable)

- Limits the number of failed login attempts before needing to wait to try again (see Note below).
- (5) "retries" are allowed, before a (60 second timeout) period has to occur, before a successful login can occur. During this timeout, "Permission Denied" will be displayed on the browser window (user name and password fields are still displayed, but you can't successfully login for 6 seconds).
- The Number of retries (5) and the time-out period (60 seconds) are set in software. They are not customer-configurable values.

## Note regarding the limit on the number of failed login attempts (at least v4.5.0)

With the web browser: The failed login attempt feature has an issue that will likely appear as normal operation, unless you are testing for "normal expected operation". The first time entering what appears to be five incorrect passwords, the login screen won't reappear for about 4-5 minutes. Then, as long as the unit remains powered-up, if the right password is entered no problem. But each time thereafter that a wrong password is typed, the login page goes away for several minutes each time. It does not reset to allowing several wrong passwords again.

Mike Sander is aware and a Mantis case has been opened. To the customer, this will appear as we are not allowing a machine to constantly hit the browser with a wrong password until the correct one is possibly entered.

## Prevention of ability to re-use password (can't re-use the last 10 passwords)

- To override any limitations on the number of times you can use the same password, either reset the password 10 times in a row, or perform a resetpw command from the front panel.

**Email from Dave L (7 May 18)** The Securesync will not allow you to use the same password again if it has been used less than ten password changes in the past. This is for security purposes.

You could keep changing the password to a different value (accept the desired password) 10 times in a row. Then an earlier

password can be re-used. The counter resets after 10 password changes.

- Even better work-around If current password is known, performing `resetpw` command from front panel or `resetpw` CLI command will automatically reset the password back to `admin123`, even if it's been recently changed less than 10 password changes (will override the "remember" of not allowing password re-use before 10 other passwords have been used).

Try the `resetpw` command from the CLI first and see if that works best.

## Report of an issue with resetting the password back to a previous value

### (v5.9.0 update) Fix to the password not being able to be re-used, for the last 10 passwords

- Per the v5.9.0 Release Notes "Repaired password reuse limitation to cap reuse failures at 10 attempts"

## Refer to JIRA ticket SSS-466 (May 2018)

### More recently split off to SSS-891 (April 2020)

email from Dave Lorah (7 May 18) referring to SF case 163235

Hello Ryan and Apps,

Morgan Stanley is having some trouble resetting the password on one of their v5.7.1 Securesyncs to a password that was used previously. I had them try the `resetpw` command and also change the password 13 times over but no success. You can see the actions in the email train below.

I believe the Securesync stores the last 10 passwords in a register and will not allow duplication if the password is in that table, is this correct?

I was experimenting on our SS 10.2.192.227 and was able to break the counter. The old passwords are now able to be entered at will.

I used an unknown combination of the Chang My Password button and `resetpw` command from the CLI. I am retrieving the logs from the customer.

Please enter a JIRA case and assign engineering support to help resolve this bug.

**Reply from Paul Myers (7 May 18)** I created a ticket "SSS-466 Case 163236 - Resetting a password to one used previously" and assigned it to Ryan Johnson. NO ONE IS WORKING ON IT YET.

Is this really a bug? Does it do what was intended which is keep the user from using the same password according to the user password settings?

**Classic web browser:** If the **Tools -> Users page of the web browser, Security tab** has min password time-frame set, can temporarily decrease the min time-frame required between password changes.

- Password re-use (can't re-use the last 10 previously-used passwords) (see Note below).
  - **Work-around:** Can apparently keep changing the password to a different value (accept the desired password) 10 times in a row. Then an earlier password can be re-used. The counter resets after **10** password changes.

## Login password has expired

The password expiration "counter" starts when the password was last changed. Technically, a short expiration period could cause it to immediately be expired (if you were to set the expiration to 10 days and the password was last changed 15 days ago, it's now automatically expired). Once expired, the web browser will no longer allow login access and will not prompt you for the old/new password (**Access Denied** is displayed). However, login with either telnet or SSH and either of these connections will prompt you for the old and new passwords. Then, you can log back into the web browser using the new password.

Or, use the `resetpw` command to reset the Spadmin password via the front panel RS-232 SERIAL port or the keypad/LCD. Then, you can login using the `spadmin123` password.

**Note:** Starting in version 5.2.1 (~~Apr 2015~~) `resetpw` also sets **LDAP and Radius to "Disabled"** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026 Update- this change was inadvertently left out of the v5.2.1 release. It will need to be added in with the next release (5.3.0?)

When resetpw is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled after performing a resetpw.

- The Serial command to reset the password via the RS-232 Serial port is “resetpw”
- Front panel keypad admin account password reset is via the System -> Cmd menus

**Note:** With Archive Versions 4.8.1 and below installed, a minor bug causes “**Not Supported**” to be displayed in the LCD after performing resetpw command, even though the command did reset the password.

### Fields are grayed-out when logged into a User account

There are two different permission levels (referred to as “Groups”) available to choose from for each User account that is created in the SecureSync- these are the “admin” and “user” groups. When “user” is selected, fields are grayed-out on several pages due to not having privilege to edit all the fields in the web browser.

Below is a screenshot for the **Tools-> Users** page of the browser, showing how to initially assign (or change thereafter) permissions for each User account that is created:

The screenshot shows a web interface titled "USER SETUP". At the top, there are three tabs: "Create User Account" (highlighted in orange), "Manage (2) User Accounts", and "Security". Below the tabs is a form with the following fields:

|                  |        |
|------------------|--------|
| Username         | kwing  |
| Password         | •••••• |
| Re-type Password | •••••• |
| Group            | user   |

The "Group" dropdown menu is open, showing three options: "user" (selected), "admin", and "user". Below the form are two buttons: "Submit" and "Reset".



## “Rules” for creating/editing passwords

- **Max length (newer browser):** Password can be up to 50 characters long (set limitation of the web browser- not a limitation of Linux).
- **Min length (newer browser):** By factory default, password minimum length is 8 characters, but this value can be changed via the “Security Policy” settings (as discussed further below).
- **Inability to re-use an earlier password** (“**Password has already been used**” message is displayed)

**Internal reference note:** The Linux OS uses the “remember” command in PAM to store earlier-used passwords. The default Value is “13” but we change this to “10”

```
spfactory@Spectracom /etc/pam.d $ cd passwd
-bash: cd: passwd: Not a directory
spfactory@Spectracom /etc/pam.d $ cat passwd
#
# The PAM configuration file for the `passwd' service
#
#password    required    pam_cracklib.so retry=3 difok=3
#
# "remember" count must match SEC_MAX_NUM_HIST_ENTRIES in
# /usr/src/spectracom/accesslibs/security.c,
password    required    pam_unix.so shadow md5 remember=10
```

This message is displayed if trying to re-use an earlier account password that has been used within the last 10 password changes.

“remember=10”

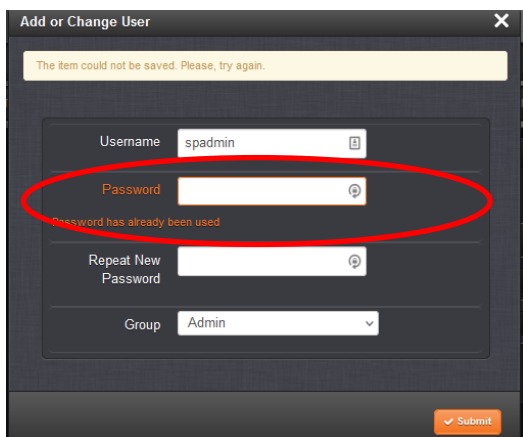
## Password Re-use/Password History

- Unit remembers the last 10 spadmin passwords created.

### Reset the spadmin password history (doesn't work in version 5.8.9 and below)

- Perform a **resetpw** command from the front panel keypad or **resetpw** from CLI interface (after login)

*Test below from v5.9.4 (shown after entering an earlier password and then pressing Submit)*



```
spadmin@Spectracom ~ $ version
Software      5.9.4
Timing System 3.6.1
Build Time    Oct 22 2021 13:06:16
spadmin@Spectracom ~ $ resetpw
spadmin@Spectracom ~ $
```

After typing **resetpw** command, the same previously entered password was accepted

## (Applicable to versions 5.8.9 and below) password history of 10 past passwords doesn't work

- Fixed in version 5.9.0

### A) (v5.9.0 update) Fix applied to the password not being able to be re-used, for the last 10 passwords

- Per the v5.9.0 Release Notes "[Repaired password reuse limitation to cap reuse failures at 10 attempts](#)"

### B) (v5.8.9 and below)

#### Only (known) viable work-arounds to reusing a past password again

- Just performing a **clean** command, **resetpw** command, or trying to change the **password 10 times** in a row, still doesn't allow a password to be re-used!!!

#### Need to perform one of the following:

1. Update software to v5.9.0 or above.

2. Replace the CF card, altogether

or better

3. Perform a "Clean" Upgrade process (AND NOT APPLY A SAVED CONFIG BUNDLER THEREAFTER)

- Refer to Salesforce Case 188930

A) Perform a "Clean Upgrade" ("complete restore to factory defaults) to the same or different version. use the Force Upgrade and Clean Upgrade checkboxes during the "upgrade" process

B) UNLESS its known that a previously created config bundle was generated **BEFORE** the password was changed to the password desired to be re-used, do not apply a saved config bundle after performing clean upgrade!!! Instead, manually configure the Time server as desired and then replace any earlier created bundles with a newly created bundle.

**Note:** Restoring an earlier saved config bundle generated after the password was changed, will re-introduce the same issue back into the system again

```
spadmin@Spectracom ~ $ resetpw
LDAP_ProcCfgLine: Ignored command: version
LDAP_ProcCfgLine: Ignored command: nss_base_shadow
LDAP_ProcCfgLine: Ignored command: nss_map_objectclass
LDAP_ProcCfgLine: Ignored command: nss_map_objectclass
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_override_attribute_value
LDAP_ProcCfgLine: Ignored command: nss_override_attribute_value
LDAP_ProcCfgLine: Ignored command: referrals
spadmin@Spectracom ~ $
```

**Email Keith sent (16 Nov 16)** Regarding the "Password has already been used" message that you observed while trying to change the spadmin account password on the SecureSync, I have some additional information to pass along to you:

**FYI:** For security considerations, like other systems that have password protections may also limit, the SecureSync's Operating System remembers the last 10 passwords that have been used for each account. It restricts you from being able to reuse the same password again, if it's been used in one of the last 10 passwords for an account. This message indicates you are trying to change the password back to one that it remembers has already been used.

Besides performing a "clean" of the SecureSync (to reset it back to its default configuration—requiring it be fully reconfigured again), a MUCH more desirable method to use, if you wish to re-use an earlier-used password again right now, is to cycle through the password change process, using arbitrary values that you don't want to use, 10 times in a row. Then on the 11<sup>th</sup> time of changing the password again, the password can be changed to any value that it's been set to anytime in the past. This work-around allows the Operating System's stored list of passwords to be cleared of the desired password to use, leaving it with the list of passwords that aren't intended to be used anytime in the near future!

Q My Customer prefers this to be 24, not 10 (as in /home/spectracom/default/etc/pam.d/passwd).

1) Is this configurable somewhere? (It wasn't obvious anywhere).

**A Keith's response:** Password requirements which can be changed/edited are "**Password Security**" under **Management->Authentication->Security Policy** page of the browser to change password requirements.

'Remember' for password history is set to 10 and cannot currently be edited. However, I am forwarding your customer's desire to be able to change it over to the Product Manager for consideration of possibly changing this in a future software update.

2) The text within /home/spectracom/default/etc/pam.d/passwd indicates the history is to match SEC\_MAX\_NUM\_HIST\_ENTRIES in /usr/src/spectracom/access\_libs/security.c. Where is this file (if, by some chance the ...pam.d/passwd file can be updated)?

**Keith's response:** NO. This file can't be updated.

---

### Password Change Attempt Logging

#### auth.log (/home/spectracom/log/auth.log)

Q Is this treated differently between execution by a privileged (admin) user against another account vs. self-update by a given account?

**A Keith's response:** NO. It's not treated differently.

### Special character/symbol limitations for passwords:

#### A) Using the newer black background web browser to create/edit password

- All keyboard characters and symbols are now accepted. Can use all special characters, such as the following: ! @ # \$ % ^ & \* ( )

#### B) While using the classic interface web browser to create/edit password,

- Just like in software versions 4.8.9 and below, installed packages related to the web browser limit the use of special characters.

The list of allowed special characters is: ~ @ # % ^ & \* ( ) \_ - + = { } [ ] ; < > . |

The following special characters are **NOT** allowed to be used when creating or editing password via the "classic interface" browser (or in versions 4.8.9 and below) : single quote ("), double quote (""), dollar sign (\$), comma (,) , backslash (\), exclamation mark (!), and apostrophe (')

**Note:** This limitation of special characters was due to the PAM or Pamecea packages we used with the earlier version of Linux. These package are not used in the newer version of linux

**Note:** Can create a password using any special characters via the new browser and be able to successfully login to the classic interface with those credentials. Just can't create the credentials in the classic interface



---

## Web browser (HTTP/HTTPS) SSL / Enhanced security / login accounts / banner

### Network port numbers for the web browsers (443 for HTTP, 80 for HTTPS, and 8080)

#### 1. Newer black/charcoal browser (v5.1.2 and above)

|     |     |           |                  |
|-----|-----|-----------|------------------|
| TCP | 443 | HTTPS/SSL | Not configurable |
| TCP | 80  | HTTP      | Not configurable |

#### 2. Classic interface web browser

- Accessible via **Port 8080**
- In addition to port 8080, the classic UI is only accessible through HTTPS (not available via HTTP).

---

### A) Classic interface web browser (white background)

#### \*\*\*Accessing the classic interface browser

##### Classic interface browser removed from product in version 5.9.0

- Per 5.9.0 Release Notes “Removed support of the Classic Web UI to increase security.”

#### In at least versions 5.4.1 and below, either:

- Open the classic interface browser via the button on the Home page of the newer browser
- Append “:8080” to the end of the address, with https in front of the address (example https://10.2.100.166:8080)

#### Classic interface disabled by factory default / removal of the “classic Interface” access button from the newer browser

- Classic browser was disabled by factory default and the access button was removed starting in update version 5.4.5
- Can still access classic interface in at least 5.4.5 by enabling it in the newer browser.
- If its desired to access the classic browser in the newer browser with versions 5.4.6 and above installed.
  - 1) Need to first enable it via the slider switch in the **Management -> Network** page of the newer browser.
  - 2) Then Append “:8080” to the end of the address in the url, with “https://” in front of the address (example https://10.2.100.166:8080)

#### Removal of classic interface browser from product

- Classic web browser completely removed in Update v5.9.0 (Jan 2021)

---

### \*\*\*Enable/disable the Classic interface browser via CLI (v5.5.0 thru 5.8.9)

- **servget** command displays status of all Services
- **servset 9 on** command enables the classic interface
- This variant of the servget/servset commands was added in version 5.5.0 update

```

spadmin@spectracom ~$ sudo seroget
Invalid arguments
Usage: seroget <service>
service: 0=daytime protocol service specified interface.
1=time protocol service intfc=0,1,2,3
2=telnet service> Set the IPv4 address and netmask for a
3=FTP service specified interface.
4=SSH service intfc=0,1,2,3
5=HTTP service addr=IPv4 address, ie 192.168.100.12
6=HTTPS service mask=IPv4 netmask, ie 255.255.255.0
7=SNMP service Display the IPv4 DNS addresses.
8=NTP service Set the primary and secondary IPv4 DNS
9=Classic UI service addresses. A missing argument will cause
the corresponding DNS address to be deleted

```

### \*\*\*Quagga account displayed in Classic Interface

In summary for customers inquiring about this account- it's a new system account added for NTP Anycast which happens to be displayed in the classic interface. But since there is no password assigned to it, there is no way to use it for login. So there are no security issues with having it present. Customers should just ignore it.

- “Quagga” is a new user account added in **version 5.2.0** to add the NTP Anycast mode function to the newer web browser.
- This unique user account is hidden in the newer black/charcoal browser but is exposed as an “artifact” in the classic interface browser (in at least version 5.2.0 and 5.2.1), since we aren't making changes to the classic interface.
- **Note:** it's displayed in the *Tools -> Users* page of the classic interface:

| Username | Group | Password | Retype Password | Update Account           | Remove Account           |
|----------|-------|----------|-----------------|--------------------------|--------------------------|
| spadmin  | admin |          |                 | <input type="checkbox"/> | <input type="checkbox"/> |
| quagga   | admin |          |                 | <input type="checkbox"/> | <input type="checkbox"/> |

- **Internal use only** (v5.8.9 and below) This user account can be used in the classic interface and can be assigned a password, if desired. But we don't.
- Ron Dries confirmed that this account can't be used to login to either of the two browsers without a password being assigned and the correct password being entered (not a security weakness).
- As long as NTP over Anycast is not being used, Quagga account can theoretically be removed via the Classic interface web browser (Tools -> Users page).

| Username | Group | Password | Retype Password | Update Account           | Remove Account                      |
|----------|-------|----------|-----------------|--------------------------|-------------------------------------|
| spadmin  | admin |          |                 | <input type="checkbox"/> | <input type="checkbox"/>            |
| quagga   | admin |          |                 | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

- Once the account has been removed, it can still be added back in via the classic interface, if needed for NTP over Anycast. But once the software is updated to one without the classic interface present, this user account can't be recreated once it's deleted.

---

## A) Newer browser (black/charcoal browser starting in v5.1.2)

### Failed password attempts/Lock placed on browser (and CLI) after failed browser logins

Per Keith- After talking with Stuart (12 Dec 2019) after three failed account login attempts (CLI or web browser logins), a 60 second lock is asserted on that account. Once this lock has been set, and after at least a full 60 second wait, users are given just one failed attempt (instead of the normal three) before another 60 second lock is placed again.

If another login attempt occurs before the full 60 second lock has elapsed, that allowed attempt is automatically failed, and so the user must wait at least another 60 seconds before attempting login again. After each failed login attempt, the failed login account counter is incremented.

He said this applies to both the SSH and web browser connections. So a failed ssh login with an account requires at least 60 seconds before using the same account to try logging into the browser.

In summary, if the wrong login password is initially issued twice, make sure to wait at least 60 seconds before trying to login again, to prevent additional failed logins just due to trying to login too soon.

---

## \*\*PC Browser requirements

### \*\*\*Java to run Javascript

**Requirements to use the newer black/charcoal web browser** (software versions 5.1.2 and above)

- The newer browser requires **Java** be installed on the PC and be working correctly in order to run Javascript in the browser
- Note the newer browser does not use/require Flash.

## Javascript

- For general and Javascript version info, refer to: <http://en.wikipedia.org/wiki/JavaScript>
- Javascript is not a package installed in the SecureSync. It consists of library files with their own versions.

Q (from Masataka with TOYO) User manual include following description as condition of control PC.

HTTP, HTTPS Servers: For browser-based administration, configuration and monitoring using Internet Explorer 7 or higher with JavaScript support, Mozilla Firefox 3 or higher (per RFCs 1945 and 2068), with JavaScript support. Could you please let us know which version of Javascript supported?

**A. From Keith** The answer is the Javascript version is web browser dependent. So the answer to your question isn't a version number. The answer is what browsers does SecureSync support. The SecureSync supports Chrome, Firefox and newer versions of Internet Explorer (we recommend IE versions 10 and above only).

## jQuery (This is a java script that renders the web UI)

### CVE-2012-6708 - Medium Severity Vulnerability

- Refer to JIRA SSS-1178
- Refer to Salesforce Cases such as 270076 (excerpt below)

Our customer from Yale University has discovered a Vulnerability with the outdated Java web console web application UI jQuery 1.7.2 This is a java script that renders the web UI.

Their Acutenix security software scan identified the problem. The scan reports it is using this library that can be accessed to send malicious files. The jQuery is like version 3 now.

They are using v5.8.9 firmware.

For now he has used access restriction to limit accessibility for mitigation.

Possible issue I found on the interweb:

### CVE-2012-6708 - Medium Severity Vulnerability

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

---

### \*\*\*Adobe Flash

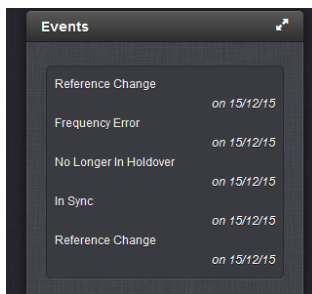
#### Impact on decommissioning Adobe flash

- Refer to Salesforce Case 244648
- Adobe Flash is not used in our products

**Email from Edouard BERTOLINI (3 Sept 2020)** I asked to engineering. They checked our codes and concluded there were no Flash applications in our products

---

### \*\*\*PHP



#### What is the installed version of PHP?

If a customer happens to ask about our PHP version, we do not install PHP in our NetClocks or SecureSync. (PHP is a type of scripting language, like Pearl, for creating web browser pages).

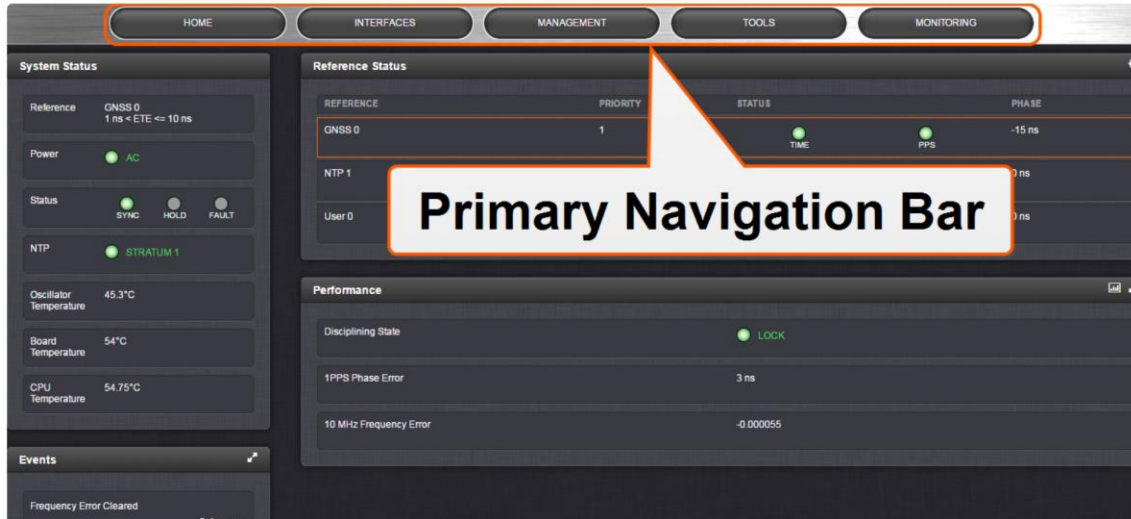
- For version information on the packages we use, refer to: [\\eng-server\projects\Brutal-2.5\sources](#) ?

## Potential vulnerabilities associated with PHP

### 1. CVE-2020-7068

- Found in v5.9.1
- Refer to Salesforce Case 258597 and JIRA ticket SSS-1125

## \*\*\*Home page of the newer browser



### Events window on Home page

- Events window displays only the most recent entries

Entries displayed are future dates and don't update (in the example above, the entries are for 2015, in 2014) If the unit is manually set to a future date, these "future" events will become the "most recent" events, until the date/time passes those events that occurred "in the future". So the future events will continue to be displayed.

In at least version 5.1.7, deleting the logs does not restore the Events window to "real time" events being displayed. To allow the Events window to show "real time" events again, until this issue is addressed, it looks like the system needs to be cleaned. Refer to Mantis case 2948.

What should fix the "future" dates being displayed- once Mantis case 2948 is fixed: Delete all the logs (no need to perform a full system clean). Logs can be deleted in the **Management** -> **Log Configuration** page of the browser. On the left side of the page, click on "**Clear all Logs**". This will clear the logs and the Event window of all of the "future" events.

## \*\*\*Customization of the newer browser

- Newer browser can be customized with a custom logo ("logo.png" file) custom language ("Locale" directory) and or custom contact info ("contact-example.html" file)
- Custom items such as a logo, locale or contact info are placed in the **home/spectracom/customize** folder (spadmin has access to this folder)

**Default contents of this folder (shown with v5.3.1 software installed)**

```
spadmin@Spectracom ~ $ cd customize
spadmin@Spectracom /home/spectracom/customize $ ls
Locale  contact-example.html  logo.png
spadmin@Spectracom /home/spectracom/customize $
```

---

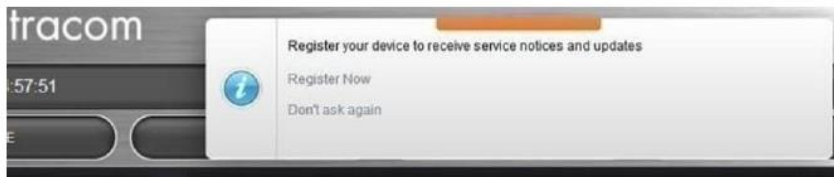
### \*\*\*Product Registration reminder / register your product

- **Website address to register a Spectracom product:**  
<http://register.spectracomcorp.com/?ProductFamily=SecureSync&SN=ENG-1208>

Q. (email from Mark Day) I have had an unusual customer comment, they have registered their unit however they are still getting the notifications asking them to register the unit. Is there a way to confirm the registration and to stop the notifications?

**A. Reply from Keith (11 May 15)** The SecureSync has no way to detect whether a customer has already registered it on our website. So they can just acknowledge that it's been manually registered. We originally discussed the SecureSyncs having the ability to "auto-register" and "auto-detect software updates being available. But these require it being open on the Internet. Many of our customers install them on closed networks isolated from the Internet. So these capabilities wouldn't work. Therefore, we decided not to spend time incorporating these specific functions.

When a customer sees the pop-up reminder in the browser to register, they can simply acknowledge the reminder, they can simply click on "Don't ask again" in this pop-up.



#### Known issue with registratration reminder

- Version 5.4.1 continues to display reminder even after selecting "don't ask again"
- Fixed in update version 5.4.5

---

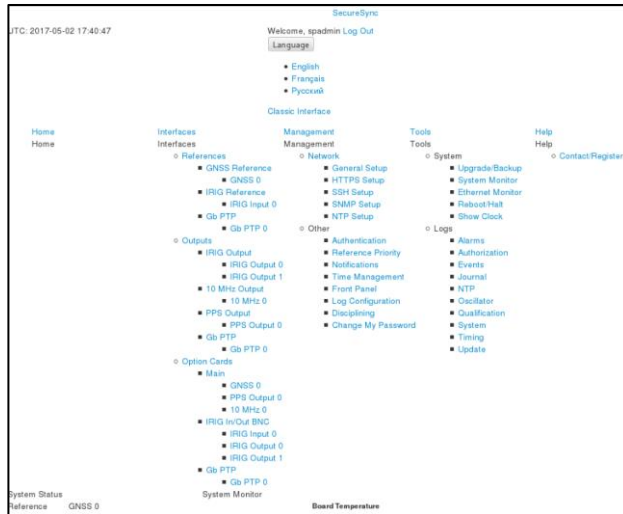
### \*\*\*Desire to create scripts for the web browser interface

- Browser itself can't be scripted- need to use the REST API interface
- REST API interface allows scripting of everything available in the web browser interface
- Refer to the REST API section of this document: [\\*\\*\\*\\*secure REST API interface \(alternate to using the standard web browser or CLI\)](#)

---

### Corrupt black/charcoal browser display (looks like an "outline" format with just words)

- Can successfully login to the newer browser in 5.1.2 and above, but the display just shows words and categories
- Refer to Salesforce cases such as 25213



**Fix: This customer reinstalled the same version of software (5.6.0) which was already installed. Problem disappeared!!**

**Email from Dave L (3 May 17)** We would like to suggest performing the 5.6.0 update again but this time use the “Perform Upgrade”, “Force Upgrade” and “Clean Upgrade” (update options all checked)  
**Customer’s reply** I went reload the 5.6.0 update and the detailed interface is working now. I am not sure what needed to settle after a factory reset and a software upgrade, but it appears to be working now. I am going to configure it and reboot a couple of times just to make sure it is solid.

### Prevent login simultaneously from multiple locations for newer (black/charcoal) browser

- Refer to JIRA case **SSS-604**
- update version 5.8.5 increased browser security
  - *Per version 5.8.5 release notes* “Improved security of the Web UI by preventing simultaneous login from multiple locations, preventing Cross Site Request Forgery (CSRF), and reducing access to the factory account.”

**Per v5.8.5 Eng Release** “[SSS-599] - Prevent Cross Site Request Forgery (CSRF) attacks”

### Cross Site Request Forgery (CSRF) for newer (black/charcoal) browser

(cross-site)

- Refer to JIRA case **SSS-599**
- update version 5.8.5 increased browser security
  - *Per version 5.8.5 release notes* “Improved security of the Web UI by preventing simultaneous login from multiple locations, preventing Cross Site Request Forgery (CSRF), and reducing access to the factory account.”

**Per v5.8.5 Eng Release** : “[SSS-604] - Prevent login simultaneously from multiple locations”

---

## \*Cookies for classic/newer browsers

- For info on enabling cookies, refer to: <https://kb.iu.edu/d/ajfi>
- Cookies do need to be enabled for the newer web browser.
- Update version 5.2.0 added a note being displayed if cookies are not enabled in the browser.

### Cookie fields

#### Name

- Name= spectracom (cookie for new browser)
- Name = PamaceaSID (cookie for classic interface browser)

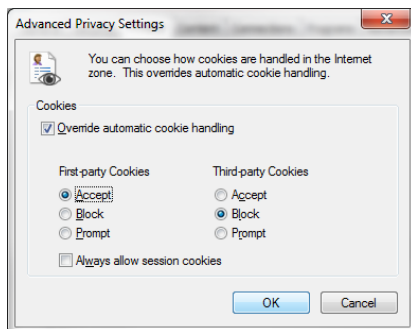
**Content** = Session ID

**Host** = IP address of time server

If cookies are blocked/disabled, the login page will report “certificate error” near the IP address and will just keep clearing the login name (won’t allow access to the browser)

## A) Internet Explorer:

- Enable “First party Cookies” in Tools -> Internet Options, Privacy tab, Advanced button:



**Important note:** Also make sure the time server is not listed as a “Site” which is configured as “**Always blocked**” (this will block cookies for just the time server, even if cookies are enabled in the Advanced button) .

In **Tools** -> **Internet Options**, **Privacy** tab, press the **Sites** button. Can optionally add the time server to the list of Sites as “**Always Allow**” if desired (this step isn’t required but doesn’t hurt to do).

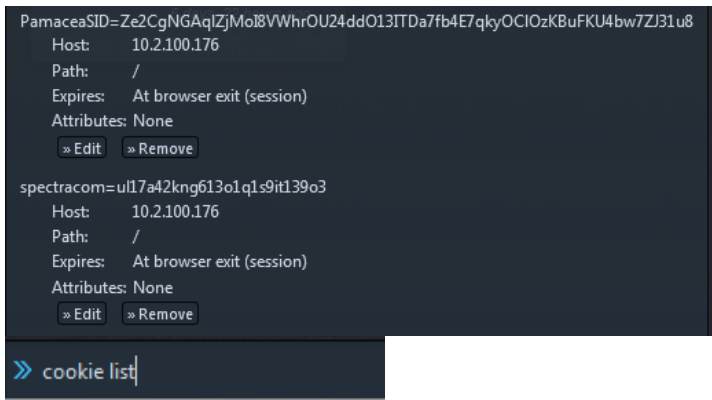
## B) FireFox

Enable “First party Cookies” in **Tools** -> **Options**, **Privacy** tab, **History** drop-down

To allow sites to set cookies on your computer, select **Accept cookies from sites**. To specify which sites are always or never allowed to use cookies, click Exceptions.

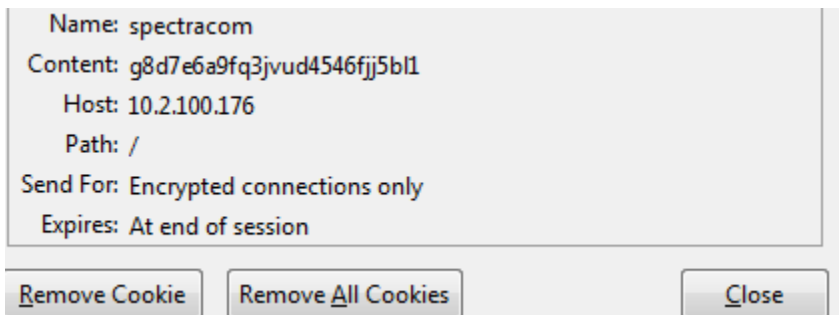
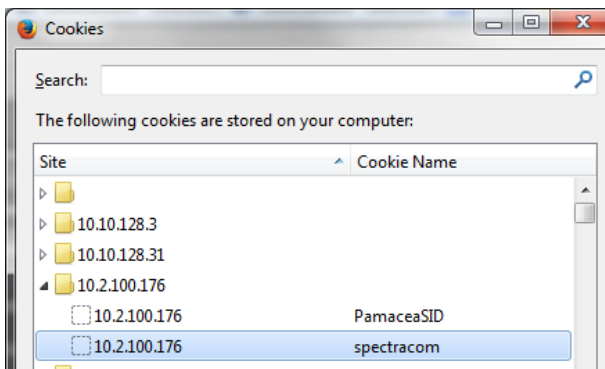
To view or remove individual cookies, press **Shift** and **F2**. At the arrow that appears at the very bottom of the page, type **cookie list** <enter> (as shown below)





Browse to the web browser and login.

Then go to **Tools -> Options -> Privacy**. Change “**Remember History**” drop-down to “**Use Custom Settings for History**”. Now click on “**Show Cookies**” and select the applicable IP address of time server. There will likely be a “**Pamacea**” cookie (for classic interface) and “**cookie**” for newer browser).



### “HttpOnly” and “Secure connections only” / “Encrypted connections only” cookies

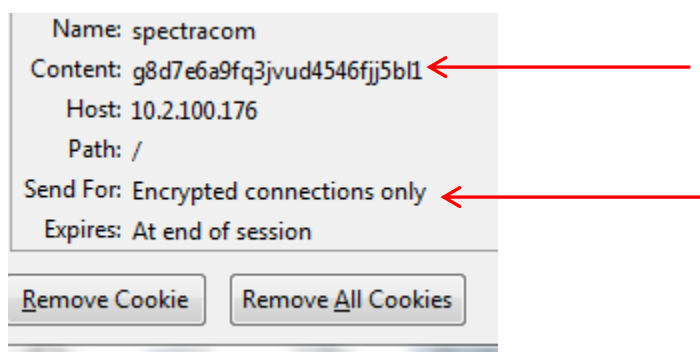
- Refer to JIRA ticket **SSS-603** (addressed in **5.8.5 and above**)
  - Per the Engineering Release Notes for v5.8.5: “\* [SSS-603] – “Set the **SECURE** and **HTTPOnly** attributes to cookies”
- Refer to Salesforce case 17412 (Justin with Wegmans)
- Refer to websites such as: [https://www.owasp.org/index.php/Testing\\_for\\_cookies\\_attributes\\_%28OTG-SESS-002%29](https://www.owasp.org/index.php/Testing_for_cookies_attributes_%28OTG-SESS-002%29)
  - Newer web browser has both **HTTPOnly** and **Secure connections only** Flags set in software (not user configurable).

**Email from Dave Sohn (16 Mar 15):** Here is the cookie from my 5.2.0 unit in house showing the HttpOnly and Secure flags

both being set. Did the cookie actually have the key "spectracom=deleted"? That usually contains the session ID. If they deleted the info before they sent it that's ok, but it is just strange. Maybe it's an expired cookie, so the flags are cleared? Not sure about that.

|                       |                                       |
|-----------------------|---------------------------------------|
| Name:                 | spectracom                            |
| Content:              | <deleted>                             |
| Domain:               | 10.10.16.20                           |
| Path:                 | /                                     |
| Send for:             | Secure connections only               |
| Accessible to script: | No (HttpOnly)                         |
| Created:              | Monday, March 16, 2015 at 11:04:43 AM |
| Expires:              | When the browsing session ends        |

FireFox cookie (from further above)



## Desire to disable Apache CBC ciphers

### A) Software versions 5.9.4 and 5.9.5

- Refer to Salesforce Case **284129**/Jira Ticket **SSS-1276**.
- Patch is available in the JIRA ticket
- Per notes in the ticket, this patch is compatible with v5.9.4 and v5.9.5. Will not be compatible with 5.9.6

---

## Concurrent sessions (Browser and CLI interface)

Q Is there any way to limit the number of concurrent sessions to both the web GUI and CLI? And is there a way to configure it to generate audit records when concurrent logons from different workstations occur?

A Concurrent sessions to the Web GUI and CLI are not configurable. Only a single user session is allowed to the Web UI. We do not have a logging mechanism for concurrent logins from different workstations.

---

## Invalidating session identifiers/session invalidated

Q Is there any way to invalidate sessions identifiers when an administrator logs out? This is referring to webUI sessions?

A. "When a user logs out of the web UI, the session is invalidated."

---

## \*Supported/unsupported web browsers and browser versions

### Supported browsers for newer black/charcoal browser (versions 5.1.2 and above)

- Chrome
- Firefox
- **Internet Explorer** (if using IE, we recommend using at least IE versions **10** and above)

**IE6:** not compatible at all with newer browser.

**IE9:** "I found all the bottoms are not visible"

**Email from Dave Sohn (17 Sept 14)** At least IE9 is required for some of our UI elements to function properly due to javascript and HTML5 requirements. We had previously looked at workarounds that emulated portions to allow the UI to run, but there were issues. This remains an open issue in our tracking system, but no additional progress has been made.

### IE8 and below

(applicable to software versions 5.6.0 and above) Internet Explorer versions 8 and below not logging in because our default signature algorithm was upgraded to SHA256 starting in 5.6.0

- Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
- An example defcert CLI syntax (5.6.0 and above only) is **defcert -sha256**
- V5.6.0 also changed the default algorithm to **SHA256** for better security (the default in 5.5.1 and below was SHA1) .
- As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access to IE8 and below

**Email from Keith (20 Jul KW)** One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can't use this newer cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

---

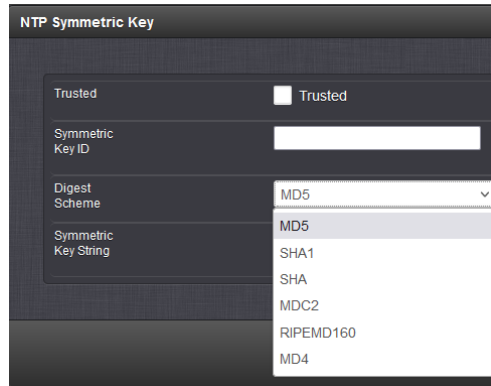
## Signature Algorithms (Such as SHA1, SHA256 and MD5)

- MD5 and SHA1 are recommended to be replaced by newer, more secure algorithms, such as SHA-256 (SHA-1 has been broken)
  - Refer to articles such as: [http://www.networkworld.com/article/3173996/security/replace-sha-1-it-s-not-that-hard.html?idg\\_eid=218d22f55abd3e2c29f91225dde70f2c&email\\_SHA1\\_lc=064024a3b5046cfb24a2b0c69fd42455f0f40e0b&utm\\_source=Sailthru&utm\\_medium=email&utm\\_campaign=NWW%20Security%20Alert%202017-02-27&utm\\_term=networkworld\\_security\\_alert](http://www.networkworld.com/article/3173996/security/replace-sha-1-it-s-not-that-hard.html?idg_eid=218d22f55abd3e2c29f91225dde70f2c&email_SHA1_lc=064024a3b5046cfb24a2b0c69fd42455f0f40e0b&utm_source=Sailthru&utm_medium=email&utm_campaign=NWW%20Security%20Alert%202017-02-27&utm_term=networkworld_security_alert)

## Support of SHA-2(SHA2)/SHA-256(SHA256) in 1200 SecureSyncs

(As of at least versions 5.9.5 and below- unlikely to ever change)

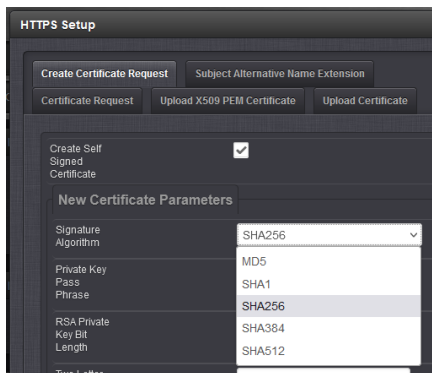
- **NTP symmetric Key:** NTP supports SHA2, but SHA2 is **not** listed/available in the drop-down field as a selection (refer to work-around further below)



Refer to Salesforce Case [300177](#)

**Per Mike Pratt (17 May 2023)** Hi Keith, you're correct that the products don't support SHA2. It's mainly just a limitation of the UI. I recently wrote an App Note regarding a workaround for this for 2400. I'll send it to you...

- **Link to referenced workaround App Note Mike Pratt created:** [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 \(Diamond\)\NTP\NTP Restriction and Authentication-MD5 and SHA](#)
- **HTTPS Certificate:** supports MD5, SHA1, **SHA256, SHA384** and **SHA512**



**List of supported ciphers list for various browser versions (such as Firefox, Chrome, Internet Explorer, etc):**

- refer to: <https://www.ssllabs.com/ssltest/clients.html>

**Example below is for IE11**

The screenshot shows a browser's user agent capabilities page for Internet Explorer 11 on Windows 7. It is divided into two main sections: 'Protocol Features' and 'Cipher Suites (in order of preference)'. The 'Protocol Features' section lists TLS 1.3 (No), TLS 1.2 (Yes), TLS 1.1 (Yes), TLS 1.0 (Yes), SSL 3 (No), and SSL 2 (No). The 'Cipher Suites' section lists 18 different cipher suites with their respective bit strengths and whether they support forward secrecy. The first suite, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384, is marked as 'Forward Secrecy' and has a bit strength of 256. Other suites include combinations of TLS\_ECDHE, TLS\_DHE, and TLS\_RSA with various key exchange, encryption, and hash algorithms.

| Protocol | Supported |
|----------|-----------|
| TLS 1.3  | No        |
| TLS 1.2  | Yes       |
| TLS 1.1  | Yes       |
| TLS 1.0  | Yes       |
| SSL 3    | No        |
| SSL 2    | No        |

| Cipher Suite                                   | Bit Strength | Forward Secrecy |
|------------------------------------------------|--------------|-----------------|
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | 256          | Forward Secrecy |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | 128          | Forward Secrecy |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)    | 256          | Forward Secrecy |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)    | 128          | Forward Secrecy |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc09f)   | 256          | Forward Secrecy |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc09e)   | 128          | Forward Secrecy |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc039)      | 256          | Forward Secrecy |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc032)      | 128          | Forward Secrecy |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0xc09d)       | 256          |                 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc09c)       | 128          |                 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0xc03d)       | 256          |                 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0xc03c)       | 128          |                 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0xc035)          | 256          |                 |

**Internet Explorer versions such as IE 11 not logging in, with no error messages being displayed**

- Refer also to the “**Enable High Security**” Checkbox section
- **IMPORTANT NOTE:** Cookies also have to be enabled. In IE- **Tools** → Internet Options → Privacy tab. Advanced button: makes sure Cookies are set to Allow/Asllow. Also in the Sites button, make sure that if the time server is listed in the Sites list, that its set to “Always Allow and not set to Always block (always block will diable cookies for this one site, and login will be denied).
- Make sure Proxy server isn't
  - In **IE- Tools** → **Internet Options** → **Connections** tab. **LAN Settings** button (“use a proxy server for your LAN” should not be selected).

Q I’m trying to use IE 11 when I try to login to the SecureSync unit with login name and password it just looks to refresh the login page and not log me in to do anything with the SecureSync unit. If I try a bad password it does give an error and I am able to SSH in and also log into the unit using Firefox and IE 10 just can’t get IE 11 to let me fully login.

**A Keith’s response (5 Jan 17):** I suspect this observation is a direct factor of a difference in the cipher list/security level setting between the two versions of IE.

I happen to have IE11 installed on my PC and I can login with no problems. In IE 11, go into **Tools-> Internet Options, Security tab**. If the **Security level** is not already set to **Medium-high**, change it this setting and then try logging in again.

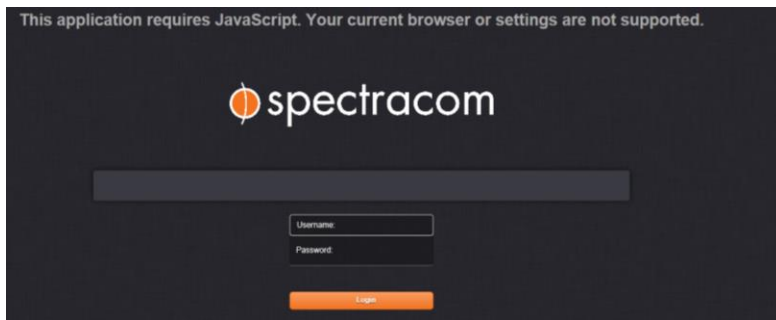
Note that when I changed my setting to high, logged-out and then tried logging back in, I can no longer login and also have an error message displayed that indicates “This application requires JavaScript. Your current browser or settings are not supported.



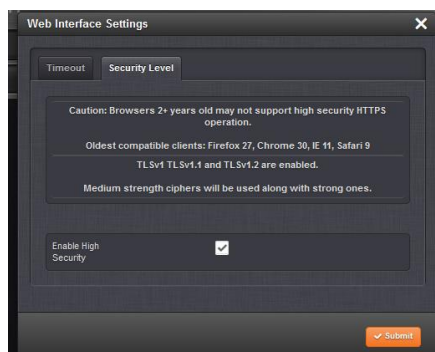
This error message is a newer one that was added in one of the more recent SecureSync software updates, specifically for this reason. I suspect your Security setting in the PC is set too high, but with an earlier software version installed, you just aren't getting the error message indicating this.

**Error message: "This application requires JavaScript. Your current browser or settings are not supported"**

**A) No successful login occurs and the following error message is displayed at the top of the window: "This application requires JavaScript. Your current browser or settings Are not supported." (as shown below)**



- If no successful login, and this error message is displayed at the top of the page, change the Security level in the PC's browser. For IE, go to Tools-> Internet Options, Security tab. If the Security level is set to High, lower it to Medium-high and then try logging in again.
- Update v5.4.5 added user selectable High and Medium level HTTPS Security settings (Management-> Network Settings page, Web Interface Settings button. Select Security Level tab in the pop-window. This window selects which list of ciphers to use for the connection with the browser.



I happen to have IE11 installed on my PC and I can login with no problems. In IE 11, go into **Tools-> Internet Options, Security tab**. If the **Security level** is not already set to **Medium-high**, change it this setting and then try logging in again.

Note that when I changed my setting to **high**, logged-out and then tried logging back in, I can no longer login and also have an error message displayed that indicates "This application requires JavaScript. Your current browser or settings are not supported."



This error message is a newer one that was added in one of the more recent SecureSync software updates, specifically for this reason. I suspect your Security setting in the PC is set too high, but with an earlier software version installed, you just aren't getting the error message indicating this,

---

## \*\*OpenSSL version installed

- Software version 5.2.0 added display of ssl version in the Tools -> Upgrade/Backup page of the newer black browser.
- Software versions 5.1.7 and below: ssl version is not reported in the browser, but is available via cli command:
- cli command to obtain the ssl version is `version ssl <enter>`  
(shown below with V4.8.8 installed)

```
[spadmin@Spectracom ~]$ version ssl
OpenSSL 1.0.1c 10 May 2012
```

---

## Determining if Apache web browser is running

Type: `ps -el | grep apache`

```
Unable to open logs
spadmin@CustService176 ~ $ ps -el | grep apache
S S      0  2177      1  0  80   0 - 32157 poll_s ?           00:01:20 apache2
S S    1001  3619  2177  0  80   0 - 32507 Sys_ep ?           00:00:01 apache2
S S    1001  6134  2177  0  80   0 - 32568 poll_s ?           00:00:03 apache2
S S    1001 23870  2177  0  80   0 - 6633  skb_re ?           00:00:00 apache2
spadmin@CustService176 ~ $
```

As shown above, there should be **apache2** in the list

---

## \*Restart HTTP/HTTPS instead of rebooting the unit (HTTPS reload command)

- There is an HTTPS “reload” command but it’s not supported in our CLI.

Perform a **servset 6 off** <enter> command followed by **servset 6 on** <enter> (as shown below). Note the two servget commands in the screenshot are optional. This will restart just the web browser service alone.

```
spadmin@CustService-176 ~ $ servset 6 off
spadmin@CustService-176 ~ $ servget 6
HTTPS Service
disabled
spadmin@CustService-176 ~ $ servset 6 on
spadmin@CustService-176 ~ $ servget 6
HTTPS Service
enabled
spadmin@CustService-176 ~ $
```

## Graceful restart of Apache browser (Graceful restart requested, doing restart)

**Note** about “[error] (9)Bad file descriptor: apr\_socket\_accept: (client socket)”

“*Graceful restart requested, doing restart*” may also be accompanied by another error log entry of “[error] (9)Bad file descriptor: apr\_socket\_accept: (client socket)” This is not a reason for the Apache restart. It is a result of the restart. Apache can apparently have trouble with a graceful restart.

Per: <https://www.linuxquestions.org/questions/linux-server-73/apache-bad-file-descriptor-593925/>

You might be hitting this bug:

[http://issues.apache.org/bugzilla/show\\_bug.cgi?id=42829](http://issues.apache.org/bugzilla/show_bug.cgi?id=42829)

I'd suggest just doing a full stop and start to get around the error until fixed. I never do graceful restarts with apache, never seems to do the job accurately.

**Email from Verizon to Dave Lorah:** I am attaching the logs of a second server that has been rebooted randomly this week at the same location.

**Email from Dave Lorah to Engineering (18 Jan 16) regarding a Verizon SecureSync:** This is a second unit in Colorado Springs that has rebooted itself. I see this message in the error log:  
[Sat Jan 16 16:26:45 2016] [notice] Graceful restart requested, doing restart

**Reply from Paul Myers (18 Jan 16)** Ron points out this is an Apache restart. We do them on occasion. This one occurs during the reboot.

Here is an online report of Apache not running after a graceful restart (until stopped/restarted). Could this be related to what this customer has reported: <https://serverfault.com/questions/780793/apache2-not-running-after-graceful-restart>

### A) Problem report: Graceful restart entry with no other associated entries in the logs. Reported loss of network connection after reboot

- Refer to case 120843

Hi Ron,

Here is an online report of Apache not running after a graceful restart (until stopped/restarted). Could this be related to what this customer has reported: <https://serverfault.com/questions/780793/apache2-not-running-after-graceful-restart>  
Today my apache instance was automatically restarted gracefully by some cron job I guess, afterwards it was not running.

Today my apache instance was automatically restarted gracefully by some cron job I guess, afterwards it was not running.

---

### HTTP login fails after logging in/logging out of HTTPS, without first closing the browser (but HTTPS login again is successful)

- Refer to Case 195013

#### (partial) customer report

- Cannot login via HTTP on chrome & can~~not~~ login thereafter (shows tacacs errors in log – the local spadmin username also does not work).
- However can login via HTTPS on chrome.
- However can login via HTTP on internet explorer.

*Below in red is a partial report generated by the Apps team (based on their NTP load testing of 5.8.4 in the lab)*  
...Regarding HTTP/HTTPS, when logging in through HTTPS then logging out - without closing your browser if you attempt to log in with HTTP you will always be rejected. If you successfully logged in through HTTPS first, then later try HTTP, this will be the case. This can be fixed by closing your browser and reopening it, using a different browser/incognito, or clearing your cookies. SecureSync will be become slower to respond under that much NTP load.



## Monitoring Services

### \*\*Watchdog (applicable to versions 5.8.9 and above, June 2020)

#### Function of Watchdog feature (per Engineering)

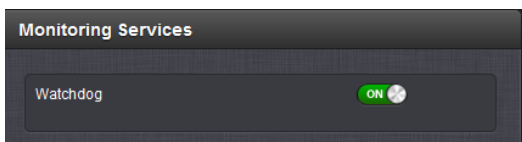
**Email from Ron Dries (27 August 2020)** Here is the response I received from Engineering:

“5.8.G introduced the ability for the system to self-recover due to a system error. The specific cause of error can be varied, however would be related to the Linux processing system. The recovery capability is handled by two levels of monitoring – one operating in the software itself, and a backup monitor that operates in hardware.

If something causes a crash in software that the software monitor is capable of detecting, the log message “System panic – rebooting” will be captured along with a special ‘crash’ log file that can aid in advanced troubleshooting. If for whatever reason something more catastrophic occurs that prevents the software monitor from capturing the error the hardware monitor will detect this and recover the system. In this case since the software is unable to operate no log message will be captured.”

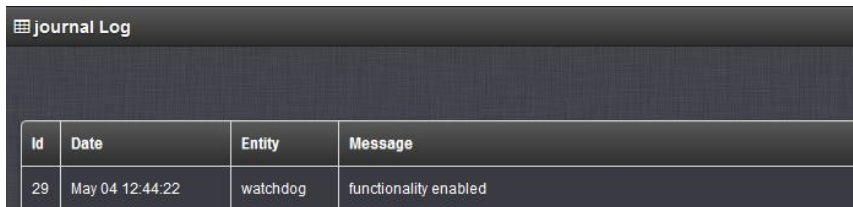
#### Browser/default configuration

- Switch added to **Tools** -> **System Monitor** page of the browser starting in version 5.8.9 (June 2020)



- Disabled by factory default/after software update to 5.8.9 (starting in 5.9.0, and above)

#### Journal log entry asserted when watchdog is enabled (“Functionality enabled”)

A screenshot of a "Journal Log" window. It has a dark grey header with a hamburger menu icon and the text "Journal Log". Below the header is a table with the following data:

| Id | Date            | Entity   | Message               |
|----|-----------------|----------|-----------------------|
| 29 | May 04 12:44:22 | watchdog | functionality enabled |

#### Associated log entries (per Engineering)

- **System panic – rebooting:** If something causes a crash in software that the software monitor is capable of detecting, the log message “System panic – rebooting” will be captured along with a special ‘crash’ log file that can aid in advanced troubleshooting.
- **Reboot with no log entry asserted:** If for whatever reason something more catastrophic occurs that prevents the software monitor from capturing the error the hardware monitor will detect this and recover the system. In this case since the software is unable to operate no log message will be captured.”

## Web browser time display (upper right corner of the browser)

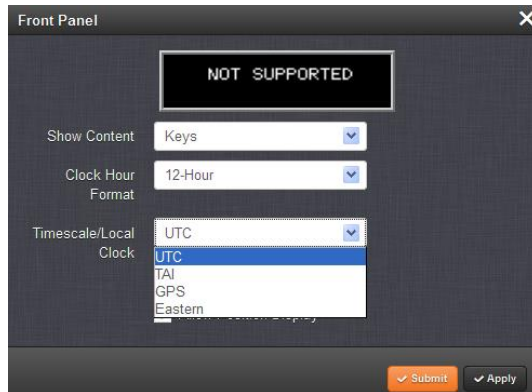
**\*\*Desire to show local time in the web browser (not possible in 9489)**

### A) Newer browser.

- Displayed time is corrected each second while connected to the time server.



Management -> Front Panel page of the browser



### B) Classic interface



#### Email from Dave Sohn on 8/23/11

“(The Time) is updated whenever the page loads or is refreshed (tested on IE, FireFox, and Chrome). However, due to network delays and when the read actually takes place, the time displayed in the UI may not match exactly the time on the SecureSync front panel display. It wouldn’t be strange to see it off by a second or more depending on the network.”

**Note:** 9489s have no front panel configuration, so it can’t be configured to show local time in the browser.

- Only available with Archive Versions 5.1.2 and above (Versions 5.0.2 and below with the classic web browser can only show UTC time in the browser).
- Web browser time display is linked to the front panel configuration (doesn’t have its own configuration).
  - The **“local clock”** selected in front panel configuration is displayed below the UTC time.
  - If **“None”** is selected, browser only shows local time. If a user-created local clock has been created and selected, this is displayed below the UTC time.

---

## Troubleshooting/known issues with local time error in web browser

### A) Web browser is showing wrong local time (just the **hours** are incorrect-minutes/seconds are correct) after 5.8.4 to 5.8.5 software update

- refer to Salesforce Cases 207355 and 207080
- Per Dave L- "The customer confirmed the front panel was showing the correct time."

### B) Web browser is showing wrong local time (just the **hours** are incorrect-minutes/seconds are correct) in versions 5.1.2 thru 5.1.7 (fixed in 5.2.0)

- Refer to Mantis Case 0002774:
- Observed in versions 5.1.2 through 5.1.7.
- Fixed in software update version 5.2.0.

After setting a local clock correctly and applying the Local Clock to the Front Panel display, the time shown in the upper left portion of the Web UI is one hour slow. Disabling DST in the Local Clock setting changes the front panel display by one hour but has no effect on the time shown in the web UI.

**Also:** Make sure the "UTC offset" in the Local Clock configuration is set for the correct offset for **STANDARD** Time (not the UTC Offset for DST time).

---

### C) Web browser is reporting the wrong time (just the **minutes/seconds** are incorrect- Hours is correct)

- Dwain Barcena w/Blue Cross saw a 20 minute error in the time display of the browser, as compared to the front panel and his Windows PC.
- While the browser is connected to the SecureSync, the browser periodically sends getTime calls to the SecureSync to keep the browser clock accurate (Ron saw this call sent a few times during just the couple minutes I was in his office)
- If the connection to the browser is broken but the page stays open (login times-out, the server is rebooted, etc) the browser can no longer get responses to the gettimes, so the browser clock will just free-run/drift off in time until a getTime call can be completed successfully again to correct the time

---

## HTTP / HSTS (HTTP Strict Transport Security)

### A) HTTP

- HTTP is not secure
- Disabled by factory default

### B) HSTS (HTTP Strict Transport Security) for HTTP

#### HSTS availability

- HSTS was added in **version 5.9.3** (Nov 2021). HSTS is NOT available in version 5.9.2 and below
  - Per v5.9.3 Release Notes: “[Added support for HTTP Strict Transport Security \(HSTS\)](#).”
  - Refer to JIRA ticket [SSS-1116](#) (Feb 2021) for request to add this feature to 1200 SecureSyncs

#### What is HSTS

Per [https://en.wikipedia.org/wiki/HTTP\\_Strict\\_Transport\\_Security](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security)

**HTTP Strict Transport Security (HSTS)** is a [web security](#) policy mechanism that helps to protect [websites](#) against [protocol downgrade attacks](#)<sup>[1]</sup> and [cookie hijacking](#). It allows [web servers](#) to declare that [web browsers](#) (or other complying [user agents](#)) should interact with it using only [HTTPS](#) connections, which provide [Transport Layer Security](#) (TLS/SSL), unlike the insecure [HTTP](#) protocol used alone. HSTS is an [IETF](#) standards track protocol and is specified in [RFC 6797](#).

The HSTS Policy is communicated by the server to the user agent via an HTTPS response [header](#) field named "Strict-Transport-Security".<sup>[1]</sup> HSTS Policy specifies a period of time during which the user agent should only access the server in a secure fashion.<sup>[2]</sup> Websites using HSTS often do not accept clear text HTTP, either by rejecting connections over HTTP or systematically redirecting users to HTTPS (though this is not required by the specification). The consequence of this is a user-agent not capable of doing TLS will not be able to connect to the site anymore.

- Refer to Salesforce Case 220401 (Jan 2020)
- HSTS module is in SecureSync, but as of at least v5.8.6, its not configured to work with SecureSync and is not available to/configurable by users (not enabled in the unit).

#### “HSTS Missing from HTTPS Server (RFC 6797)”

- Refer to Salesforce Cases such as 257254
- Refer to sites such as: <https://www.ibm.com/support/pages/resolving-missing-hsts-or-missing-http-strict-transport-security-websphere>

**Q Report from Customer:** “HSTS missing from HTTPS server. if HTTPS is in use on port 443, HSTS must be enforced. Inquire with vendor how to configure. if not possible, need vendor documentation.”

**A reply from Dave L (17 Jan 2020)** The Securesync is equipped with HSTS but this is not user accessible or configurable. You asked about documentation about this. What do you require?

Also, HSTS is not supported in some web browsers. What browser are you using to access the Securesync?

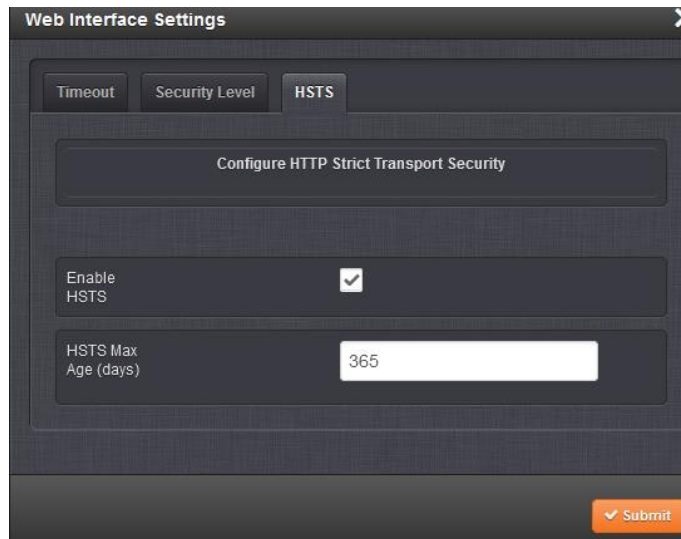
**A reply from Dave L (30 Jan 2020)** I have consulted our engineering group and confirmed HSTS is not enabled and will not function in the Securesync product. It is not capable of enabling or configuring HSTS. To enable HSTS would require a product design change.

## HSTS setup/configuration (applicable to versions 5.9.4 and above only)

- Refer to online 1200 SecureSync user guide (ex[https://orolia.com/manuals/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/HTTPS\\_Config.htm](https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/SETUP/HTTPS_Config.htm))

### To configure HSTS

- 1) Navigate to **MANAGEMENT** > **Network Setup**.
- 2) Select **Web Interface Settings** (button on left)
- 3) Select the **HSTS** tab to Enable/Disable HSTS, or to configure the Max Age of the functionality (default is set to 1 year).



For more information on HSTS requirements, refer to <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>.

### Viewing the HSTS header (when HSTS is enabled)

Per: <https://blog.nvisium.com/is-your-site-hsts-enabled>

#### Testing HSTS

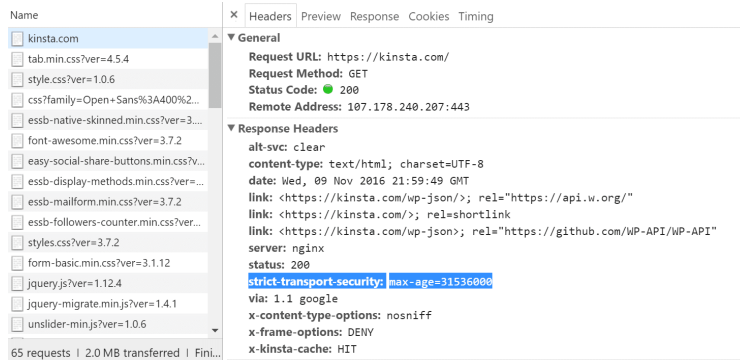
- Leverage an intercepting proxy (e.g. Burp) or browser tools (e.g. Chrome DevTools / Firefox Developer Tools) to examine server responses
- In **Chrome**, type the below to determine if a host is in your STS cache <chrome://net-internals/#hsts>
- In **Firefox**, you can use the Strict Transport Security Detector add-on to see if the site supports HSTS (<https://addons.mozilla.org/en-US/firefox/addon/strict-transport-security-d/>)
  - "PinPatrol" (Firefox Add-On)

Per: <https://kinsta.com/knowledgebase/hsts-strict-transport-security/>

### Verify HSTS Header

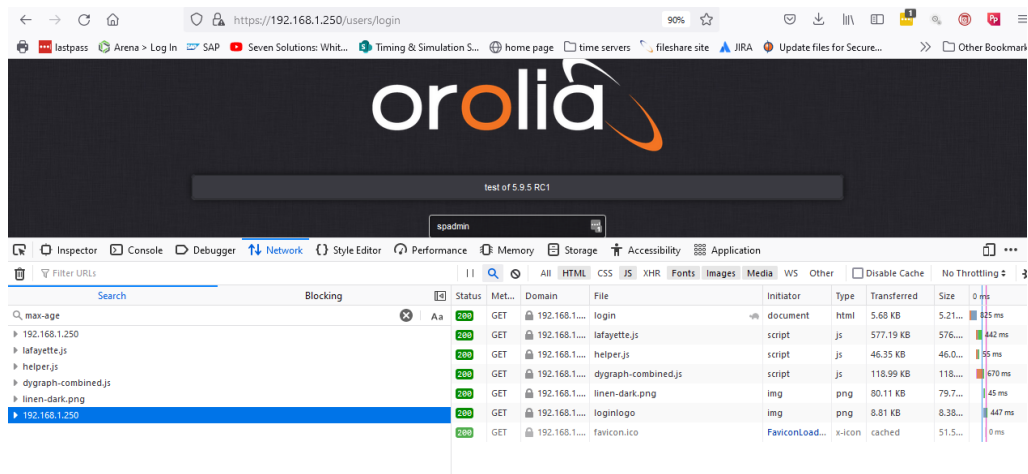
There are a couple easy ways to check if the HSTS is working on your WordPress site. You can **launch Google Chrome Devtools, click into the "Network" tab and look at the headers tab. As you can see below on our**

**Kinsta website the HSTS value: “strict-transport-security: max-age=31536000” is being applied.**

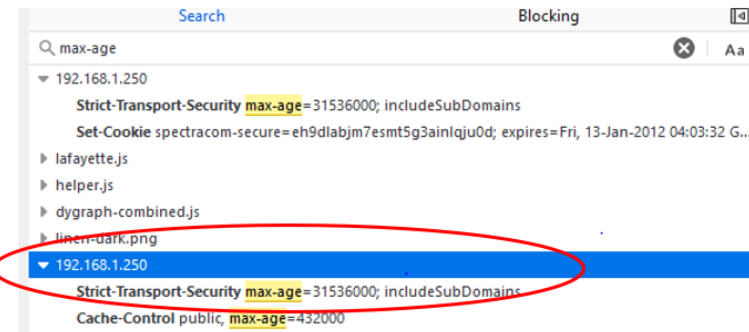


### Keith's testing: In Firefox or Chrome

1. Open a browser connection to the SecureSync
2. In Google, click the “three dots” and select More Tools -> Developer Tools  
In Firefox, go to Tools -> Browser Tools -> Web Developer Tools
3. Select the “**Network**” tab
4. Click the magnifying glass and search for “**max-age**”
5. Reload the page
6. The list on the left is/are all the locations max-age (a parameter for HSTS) was found.



7. Click on the item(s) listed on the left to see the HSTS parameters (**Strict-Transport-Security max age**) drop-down below it.



**HSTS is enabled in web browser, but not being detected (v5.9.4, and apparently 5.9.5 pre-release. Fixed in 5.9.5)**

- Refer to Salesforce Case 284393 (May 2022: observed with 5.9.4 installed)
- Refer to JIRA **SSS-1277**
- I seem to be duplicating this on 5.9.4, both before and after a reboot.
- Believe this was fixed in the v5.9.5 released update

The following is an excerpt from internal Engineering notes about the v5.9.5 update:

5.9.5 also contains fixes to address several issues (most customer reported, one internally identified):  
- HSTS was added and can be enabled, but not working

*Per Tim Hammer (excerpt from SSS-1277): June 8, 2022 at 9:53 AM*

I confirmed behavior reported by customer & Keith Wing.

When updating from 5.9.1 (or earlier) to 5.9.4, the 000-httpd-default.conf file will be carried forward because it is included in the config transfer list.

However, we did not create a transfer script to handle the HSTS support added in the feature for 5.9.4.

Also in 5.9.4, we removed the Classic WUI code and supporting files. One of the changes resulted in the 000-httpd-default.conf file being removed from the transfer list (filelist.txt). Thus, when upgrading from 5.9.4 to 5.9.5 the file is not carried forward, the new file from the upgrade bundle is installed, and support for HSTS is in place.

**So**, there is no actual change required to “fix” this in 5.9.5.

---

## \*\*HTTPS/SSL Certificates (HTTPS certificates)

### Good references regarding SSLx509 certificates

- [https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Certificates.htm#Cert\\_What\\_is\\_it](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Certificates.htm#Cert_What_is_it)
- <https://www.openssl.org/>
- [https://www.openssl.org/docs/man1.0.2/man5/x509v3\\_config.html](https://www.openssl.org/docs/man1.0.2/man5/x509v3_config.html)

**FIPS-140 validation:** <https://www.openssl.org/docs/fips.html>

### *Below is from online SecureSync user guide:*

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/HTTPS\\_cert\\_formats.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/HTTPS_cert_formats.htm)

SecureSync supports X.509 PEM and DER Certificates, as well as PKCS#7 PEM and DER formatted Certificates.

You can create a unique X.509 self-signed Certificate, an RSA private key and X.509 certificate request using the Web UI. RSA private keys are supported because they are the most widely accepted. At this time, DSA keys are not supported.

SecureSync supports two different modes of HTTPS operation: The Standard HTTPS Level (default), and a High-Security Level. For more information, see [HTTPS Security Levels](#).

### Hashing and encryption algorithms

- Certificates define which hash to use for browser connections (such as “SHA1’ or ‘MD5’)
- Certificates do not define which encryption algorithms to select (this is determined by the **cipher lists** on the server and client)

### HTTPS certificate validity/expiry

- Spectracom default certificate is valid for **10** years.
- New certificate needs to be manually created by user when it expires.

### Supported Certificate Formats

- SecureSync supports X.509 PEM and DER Certificates, as well as PKCS#7 PEM and DER formatted Certificates.

### CAC cards/DoD PKI certificates (for Dept of Defense)

- Refer to Salesforce Case 232854 (May 2020)
- Refer to sites such as: <https://public.cyber.mil/pki-pke/>

Q is the SecureSync capable of using DoD PKI Certificates for login authentication either for the GUI or SSH login? If not, is there a plan to incorporate this feature and when?

What is a DOD PKI certificate?

A **certificate** is a digital document providing the identity of a Web site or individuals. **DoD** Web sites use a **certificate** to identify themselves to their users and to enable secure connections. ... The **DoD PKI** Infrastructure is comprised of two Root **Certification** Authorities and a number of Intermediate Authorities.



---

## Root certificate/Intermediate SSL certificates (chain certificates)

- Refer to sites such as <https://kb.wisc.edu/page.php?id=18923>
- Update version 5.6.0 (Apr 2017) added support for x509 PEM CA chain certificates

### What is a **Root Certificate**?

- A Root SSL certificate is a certificate issued by a trusted certificate authority(CA).
- A root certificate is an unsigned or a self-signed public key certificate that identifies the root certificate authority (CA). A root certificate is part of a public key infrastructure scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority.
- A root certificate is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

What Is an **Intermediate Certificate**? To enhance the security of the Root certificate, we create two intermediate certificates from which SSL certificates are signed and issued.

An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, through the intermediate and ending with the SSL certificate issued to you. Such certificates are called chained root certificates.

Q Does the SecureSync support the inclusion of intermediate SSL certificates (chain certs)? If so, how does one install them? If not, is it on the roadmap (and what's the ETA)?

## Certificate Chain (Chain certificates)

- It is also possible to upload a X.509 PEM Certificate Chain by pasting the text of the second certificate behind the regular CA Certificate.

---

## Creating a new HTTPS Certificate Request (CR)

- Refer to the online SecureSync user manual:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/HTTPS\\_CertRequ.htm?Highlight=https%20certificate](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/HTTPS_CertRequ.htm?Highlight=https%20certificate)
  - **SecureSync HTTPS doc:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\HTTPS certificate>
  - **NetClock 9400 HTTPS doc:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\HTTPS certificate>
  - **Another good online reference:** [https://www.openssl.org/docs/man1.0.2/man5/x509v3\\_config.html](https://www.openssl.org/docs/man1.0.2/man5/x509v3_config.html)
- New HTTPS certificates/Certificate requests can only be created via the web browser.
- Starting in v5.6.0, the default certificate is now created using **sha256** (it used to be created with **sha1**)
  - When a unit is updated from a version prior to 5.6.0, to versions 5.6.0 or above, the existing HTTPS certificate is carried forward (a new certificate isn't created during upgrade). A new certificate will need to be created if its necessary/desired to go to sha256 instead of the original sha1.

## A) Using the **defcert** CLI command to create new CR (Certificate Request)

- The only CLI command associated with HTTPS certificates is the **defcert** command (to reset the certificate back to default)
  - Optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - Example syntax is **defcert -sha256**

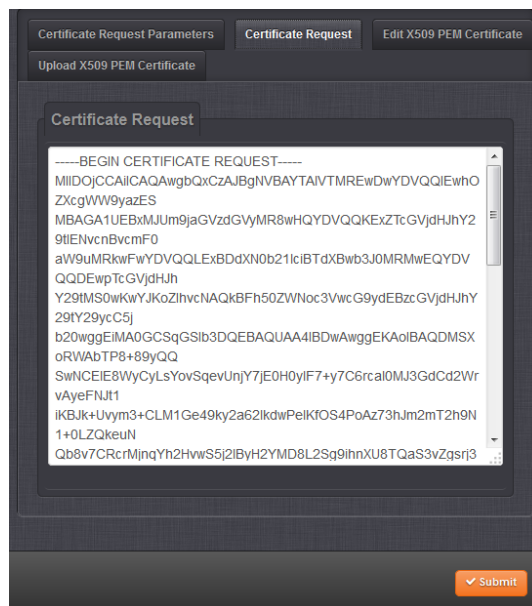
- IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).

### Note about keys for authentication and ciphers for encryption, when generating new certificates

- 1) Keys for authentication are chosen via drop-downs when the certificate is created.
- 2) Ciphers for encryption are not defined in the certificate. A cipher is selected from a list (one in both the NTP server and the client) of ciphers supported. The most secure Cipher in both lists is typically selected.

## B) Creating a new CSR (Certificate Request) using the Web browser

1. Navigate to the **Management -> HTTPS Setup** page of the browser
2. (Optional Step to be able to confirm a new certificate has been created at the end of this process): Go to the **Certificate Request** tab to view the current certificate. Either screenshot it, as shown below or copy/paste the contents to a Word document.



3. Select the **“Certificate Request Parameters”** tab.

The screenshot shows the 'HTTPS Setup' window with the 'Certificate Request Parameters' tab selected. The form contains the following fields:

- Create Self Signed Certificate:
- Signature Algorithm: SHA1
- Private Key Pass Phrase: [text input]
- RSA Private Key Bit Length: 2048
- Two Letter Country Code (ISO 3166-1): [text input]
- State Or Province Name: [text input]
- Locality Name: [text input]
- Organization Name: [text input]
- Organizational Unit Name: [text input]
- Common Name (e.g. Hostname or IP): [text input]
- Email Address: [text input]
- Challenge Password: [text input]

A callout box points to the 'Common Name' field with the text: **“Common Name” field:** See additional “Common Name” info further below regarding RFC 2818 (DNS SAN) compliancy

**Important (not applicable to versions 5.6.0 and above):** Make sure to select the **“Create Self Signed Certificate”** checkbox at the top of the page (otherwise a new certificate won't be generated).

1. Enter data in the remaining fields
2. Press Submit
3. (Optional Step to see the new certificate is being/has been created)-Click on the **“Certificate Request”** tab after submitting the data. The Screenshot below shows the new certificate request is being generated.

The screenshot shows the 'HTTPS Setup' window with the 'Certificate Request' tab selected. A yellow message bar at the top says 'The item has been saved'. Below the tabs, the 'Certificate Request' field contains the text: 'Creating new public/private keys, self-signed certificate and certificate request...'

4. Once the certificate has been successfully created, the browser connection will be lost. Log back in and navigate back to the **Management -> HTTPS Setup** page of the browser. **Certificate Request** tab.
- Note:** the larger the key size that was entered in the Certificate Request, the longer it takes for the new certificate to be created. It may take a few minutes to create the new certificate.
5. The Certificate Request field should now be different than the screenshot or copy/paste of the original certificate.

## Info regarding particular fields in the CR creation

### 1. Private Key Pass phrase” and “Challenge Password” fields

The screenshot shows the 'HTTPS Setup' window with a 'Create Certificate Request' tab selected. The 'New Certificate Parameters' section includes fields for Signature Algorithm (SHA256), Private Key Pass Phrase (circled in red), RSA Private Key Bit Length (2048), Two Letter Country Code (ISO 3166-1), State Or Province Name, Locality Name, Organization Name, Organizational Unit Name, Common Name (e.g. Hostname or IP) (48308839), Email Address, Challenge Password (circled in red), Optional Organization Name, and Self Signed Certificate Expiration (Days) (7200). A message at the top states 'The item could not be saved. Please, try again.'

- Both these are mandatory fields (can't be left blank/null)
- Refer to Salesforce Cases such as 241766 for customers wanting to leave these fields blank (excerpt below)

**Private Key Pass Phrase:** This field can normally be any value. Unless you are having a Certificate Authority (CA) create the Certificate for you (this is rare), this field is just used to help generate the new key and does not need to be “remembered” for later use.

My company does this

**Challenge Password:** Can normally be any value. Unless you are having a “Certificate Authority” create the Certificate for you (this is rare), this field is just used to help generate the new key and does not need to be “remembered” for later use.

my company does this

So I need to leave those 2 fields blank and only enter CN info. How can I get past this?

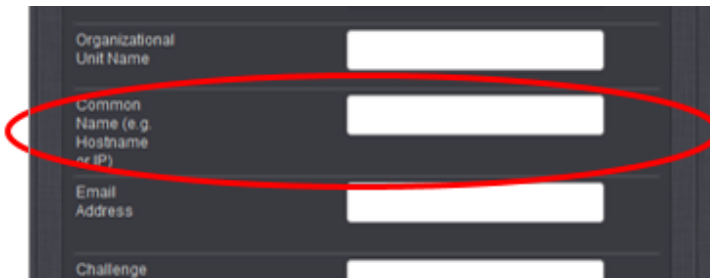
### 2. “Organizational Unit (OU)” field

The screenshot shows a form field for 'Organizational Unit Name' which is circled in red. Below it is the 'Common Name (e.g. Hostname)' field.

## CA requires multiple Organizational Unit (OU)

- This functionality not available in versions 5.7.1 and below (can only enter one OU value)
- Refer to SF case 119473 and JIRA ticket JIRA-SSS-380

### 3. “Common Name field” - Subject Alternate Name (DNS SAN) / RFC-2818 compliancy



Organizational Unit Name

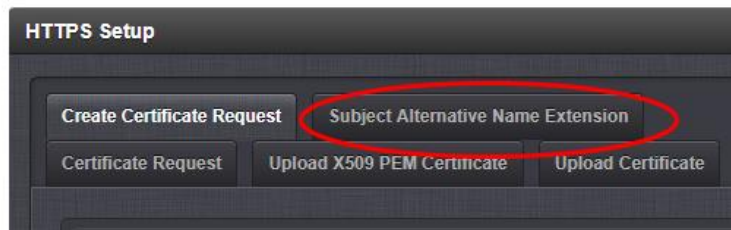
Common Name (e.g. Hostname or IP)

Email Address

Challenge

#### A) RFC-2818 compliancy / SAN Name (Subject Alternate Name Extension) / UCC Certificate (available in update versions 5.8.0 and above only)

- Refer to [https://www.openssl.org/docs/apps/x509v3\\_config.html](https://www.openssl.org/docs/apps/x509v3_config.html)
- Refer to sites such as <https://tools.ietf.org/html/rfc2818>
  - the Common name must be DNS SAN
- Ability to create SAN certificates was added in update version 5.8.0
- SAN certificates essentially allow adding more than one Common Name for the time server (standard certificate only supports one Common Name)
- Creating a SAN certificate involves configuring a second tab (“**Subject Alternative Name Extension**”) in the HTTPS Setup page



#### Multiple Domain UCC Certificate (just nother name for “SAN Certificate”)

(Note: UCC stands for Unified Communication Certificate)

- Sites about “UCC certificates”:
  - <https://www.godaddy.com/help/what-is-a-multiple-domain-ucc-ssl-certificate-3908> and <https://www.ssl.com/faqs/what-is-a-ucc/>

A Unified Communications Certificate (UCC) is an SSL certificate that protects multiple domains and subdomains.
  - <https://www.ssl.com/faqs/what-is-a-ucc/>

A **Unified Communication Certificate** (or **UCC**) is a digital security certificate which allows multiple hostnames to be protected by a single certificate.

UC certificates are also known as **Subject Alternate Name** (or **SAN**) certificates, **multi-domain certificates** or **Exchange certificates**.

- For info on creating a SAN certificate, refer to online SecureSync user guide at:  
[http://manuals.spectracom.com/NC/Content/NC\\_and\\_SS/Com/Topics/SETUP/HTTPSubjAltName.htm](http://manuals.spectracom.com/NC/Content/NC_and_SS/Com/Topics/SETUP/HTTPSubjAltName.htm)

**Caution:** Subject Alternative Names must be added before a new Certificate Request is generated, otherwise the Certificate Request will have to be created again to include the Subject Alternative Names. Any information entered into the Create Certificate Request tab that has not been submitted will be lost by adding, deleting, or editing Subject Alternative Names.

The screenshot shows a web form titled "Add Subject Alternative Name". It has three main input fields: "Type" (a dropdown menu currently set to "DNS"), "Name" (a text input field), and "Directory Name" (a checkbox). A "Submit" button is at the bottom right. Two callout boxes provide additional information: one for the "Type" dropdown and one for the "Directory Name" checkbox.

**(“Type” dropdown) select:** DNS, IP, email, URI, RID, or dirName (see additional info below)

**Directory Name checkbox:** For “Directory Subject Alternative Names” (dirName), check the Directory Name box, and additional optional fields will be available (see additional info below)

## B) “Type” drop-down

Per [https://www.openssl.org/docs/man1.0.2/man5/x509v3\\_config.html](https://www.openssl.org/docs/man1.0.2/man5/x509v3_config.html)

The subject alternative name extension allows various literal values to be included in the configuration file. These include:

- **email** (an email address)
- **URI** a uniform resource indicator,
- **DNS** (a DNS domain name),
- **RID** (a registered ID: OBJECT IDENTIFIER),
- **IP** (an IP address, can be in either IPv4 or IPv6 format),
- **dirName** (a distinguished name) and otherName.

### “Directory Name” (dirName) checkbox (to enable “Directory Subject Alternative Names”)

For Directory Subject Alternative Names (dirName), check the Directory Name box, and additional optional fields will be available:

- **Two Letter Country Code:** must match ISO-3166-1 value.
- **Organization name:** name of organization creating certificate.
- **Organizational Unit Name:** The applicable subdivision of the organization creating the certificate.
- **Common name:** The name of the host being authenticated. The Common Name field in the X.509 Certificate must match the host name, IP address, or URL used to reach the host via HTTPS.

## C) Support for SANS/RFC-2818 was added in version 5.8.0 (May, 2018) and above:.

- Per the 5.8.0 Release Note: “**Added HTTPS certificate support of SANS fields for Common Names**”
- Refer to JIRA Ticket **JIRA-SSS-372** <https://spectracom.atlassian.net/browse/SSS-372?jql=text%20~%20%22san%22%20order%20by%20created%20DESC>

- Refer to earlier Mantis case 2867 (<http://cvsmantis.int.rolia.com/mantis/view.php?id=2867>)

- Example associated Salesforce cases: 124543, 118702, 15127
- Software versions 5.7.3 and below, SAN is not supported.
- Refer to [https://www.openssl.org/docs/apps/x509v3\\_config.html](https://www.openssl.org/docs/apps/x509v3_config.html)

**Email Keith sent to Engineering** I'm not aware of SecureSync currently being able to support Subject Alternate Names (SAN) SSL certificates ([https://www.openssl.org/docs/apps/x509v3\\_config.html](https://www.openssl.org/docs/apps/x509v3_config.html) ). But I wanted to confirm this before responding. I was wondering if it's possible to create SSL signing requests with subject alternate names? There doesn't seem to be any field for this value within the certificate generation utility provided within the web GUI.

- Refer to sites such as <https://tools.ietf.org/html/rfc2818>
  - the Common name must be DNS SAN

### Q Is SecureSync RFC 2818 compliant?

I am asking does your screens allow us to add a DNS Subject alternative Name(DNS SANS). <https://www.chromestatus.com/features/4981025180483584> It is now being enforced by google chrome, and eventually by all browser vendors.

**Note:** Questions/Answer/info below are for all versions prior to v5.8.0 (before SANS support was added in 5.8.0)

**A Per Keith (26 Sep 17)** Apparently not (in update versions 5.7.1 and below ...)

- (26 Sep 17) Per Paul M: "JIRA-SSS-372 is created and assigned to Ryan Johnson"

**Note:** As indicated below, this inquiry (case 118702) was due to Chrome browser:

Q Dave L to Paul (26 Sep 17) Cigna is looking to be compliant with the RFC2818 and had a comment about out Certificate Request setup in the SecureSync's web UI. They said we are missing a "Subject Alternative Name" field and this makes it difficult to generate a valid Certificate Request. This could be added in the next firmware update?

**A Reply from Paul to Dave L (26 Sep 17)** You are correct we will have to deprecate and remove use of COMMON NAME for SAN Subject Alternative Name.

I had believed we WERE basically compliant to RFC 2818 by accepting a single fully qualified domain name (FQDN) due to current practices of using the common name...

However, it appears I am wrong now. RFC2818 when properly read and implemented calls for dropping support of COMMON NAME for SAN (Subject Alternative Name) except NO ONE DID IT for the last 17 years.

Google Chrome 58 stable in April 2017 finally initiated this long overdue change likely because it is being exploited.

<https://www.thesslstore.com/blog/security-changes-in-chrome-58/>  
<https://productforums.google.com/forum/#!topic/chrome/-19ZxwjaCjw>  
[https://en.wikipedia.org/wiki/Subject\\_Alternative\\_Name](https://en.wikipedia.org/wiki/Subject_Alternative_Name)

The Subject Alternative name appears to be referenced/defined in RFC 5280  
<https://tools.ietf.org/html/rfc5280#section-4.2.1.6>

### Reported bug in SW V5.9.4" (new certificate request under HTTPS Setup, creates new line in "Subject Alternative Names)

"We noticed a new bug in version 5.9.4. If you create a new certificate request under HTTPS Setup, it creates a new line in "Subject Alternative Names", when the line already exists. This causes new cert requests on the CA side to fail. It should probably check if the alternative name exists and not add it if it does. Please let me know if you need more details."

- Reported July 2022
- Refer to Salesforce Case 286588/JIRA ticket SSS-1288



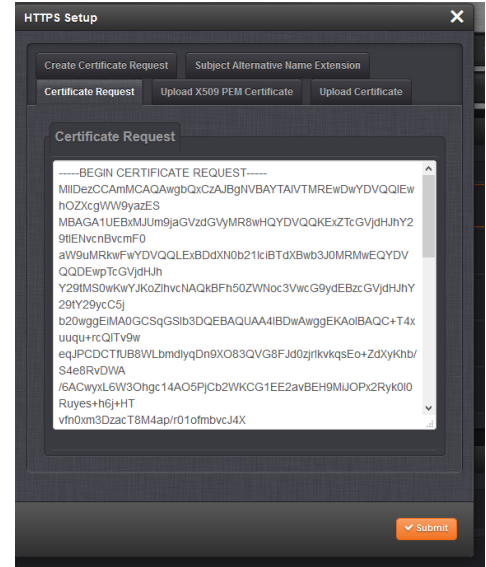


**B) server.csr file (this is the Certificate Request / "CR" file)**

**cat server.csr** (as either spadmin or spfactory)

```
spfactory@Spectracom /etc/ssl/apache2 $ cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDezCCAMCAQAwgBQxCzAJBgNVBAYTA1VTMREwDwYDVQQIEWh0ZXgW9yazES
MBAGA1UEBxMjUm9jaGVzdGVyMR8wHQYDVQKExZTcGVjdHJhY29tIENvcnBvcnF0
aW9uMRkwFwYDVQQLExBDbDdXN0b211ciBTdXBw3J0MRMwEQYDVQDEwPjTcGVjdHJh
Y29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJhY29tY29ycC5j
b20wgqEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQC+T4xuuiu+rcQ1T9v9
eqJPCDCTUB8WLBmdlyqDn9X083QVG8FJd0zjrIkvkqsEo+ZdXyKhb/S4e8RvDWA
/6ACwYxL6W30hgcl4AO5PjCb2WKCg1EE2avBEH9MiJOPx2Ryk0I0Ruyes+h6j+HT
vfn0xm3DzacT8M4ap/r01ofmbvcJ4X/m0enuL1SqNuF0cCFVnTmRlUGv9kDAMv1J
EfrsWkKsWZrakgWOMUK4qY/nfdZeicm/CIIdppVkiP2/vdrM/FeBxxQkLqU/4K16
tB2o6z2VA6m4Xg2xmdQiguOTNylQM2sALVz+PKg/FrZisJrGdO14DjYRU6uB414
ydiPAGMBAAGggYAWGQYJKoZIhvcNAQkCMQwTC1Nw2WN0cmFjb20wIwYJKoZIhvcN
AQkHMRYTFEx1Z2FsbH1UcmFjZWF1bGVuUa11MD4GCSqGSIb3DQEJJDExMCM8wCOYD
VR0TBAlwADALBgNVHQ8EBAMCBeAwFQYDVRORBAA4wDIKU3B1Y3RyYWNvbTANBgkq
hkiG9w0BAQsFAAOCAQEAFjZhQNh5mi/csDsW0lhd1H/oy3PnbjNLvsA7Q9NhXMGp
ZeyrkUpvcOTDU/hf/oyDHso3d6E9PdmBBGwiWhRjG3Ys1Q9HnXkfI0EhXozSW0
4kKRqP2vd9GRBK6nyQLJlFfSFdKIXBF540g2LUmRyPYwpSlnov1a3WqLope5yNSi
AzKuisaY45Q13mMq1LN2qNpsylv0mejp9OFHSH/Rhr2G+fluPhoUIx+bavGKbsq9
thWBpdMSZrQBaxz1RfKoc+LzWswyYINpRCNMocQAXpblvI9yDx4Vzx4sqDpKwAV
OsyDNFeJlrIPvtjIiK0BUQPcOns6Uqjz2P2wilbFIg==
-----END CERTIFICATE REQUEST-----
spfactory@Spectracom /etc/ssl/apache2 $
```

**Management -> HTTPS Setup page**



**C) server.key file (this is the private key file which has to remain inside the SecureSync)**

**cat server.key** (as either spadmin or spfactory) "Permission denied"

```
spfactory@Spectracom /etc/ssl/apache2 $ cat server.key
cat: server.key: Permission denied
spfactory@Spectracom /etc/ssl/apache2 $
```

**D) server.pem file (this is the file**

**cat server.pem** (as either spadmin or spfactory) "Permission denied"

```
spfactory@Spectracom /etc/ssl/apache2 $ cat server.pem
cat: server.pem: Permission denied
spfactory@Spectracom /etc/ssl/apache2 $
```

**Issues observed after installing the CERT**

**A) Customers often install a "generic" CERT that was not generated from the Certificate Request (CSR) generated in/extracted from the SecureSync (or install the same Cert on more than one SecureSync)**

1. This corrupts HTTPS (it stops working)
2. All PC's display will likely show an error message, such as "This site can't be reached"
3. Login to the CLI interface (telnet or ssh) and type: **defcert**
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.  
Example syntax is **-sha256**
  - V5.6.0 also changed the default algorithm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).
4. Perform an **unrestrict** CLI command

5. Perform a **servset 6 off** and then a **servset 6 on**

**Slightly modified Email Keith sent to help troubleshoot (15 May 2020)** “This site can't be reached” is a very generic message, that the PC can't reach the SecureSync over the network. It doesn't appear this message is related to the HTTPS certificate, especially if it's the only message displayed. (no certificate error messages being displayed).

Some questions for you:

- 1) Was the PEM certificate generated directly from the Certificate Request (CSR) first created/extracted from the SAME SecureSync the certificate was installed in Note this is absolutely essential. Installing a “generic certificate not generated from the Certificate Request (or installing a cert in a different SecureSync than the SecureSync that the CSR was generated in) will corrupt HTTPS. The “invalid certificate needs to be deleted for HTTPS to work again.
- 2) What browser app (and its version) are you using on this PC to connect (such as Internet Explorer, Firefox, Chrome, etc)?
- 3) To confirm is “This site can't be reached” the only message being displayed?
- 4) Is this PC on the very same subnet as the SecureSync? or, are there any routers/firewalls in between?
- 5) Was it verified that this same PC was able to login to the SecureSync's browser JUST before copy/pasting the new PEM certificate into the SecureSync?
- 6) Can you connect to the SecureSync's web browser from this same PC, using a different browser app installed on this PC (if you are currently using Internet Explorer to try to connect, can you connect to the SecureSync using Chrome or Firefox, for instances)?
- 7) Can you still connect to the SecureSync's web browser from any other PC on the network?
- 8) Can you access/login to the SecureSync's CLI interface (via an ssh session) from this same PC displaying the error.

Let us know the answers to the above questions and then we can go from there.

---

**“Accept” the new certificate in each PC, the next time the PC is used to connect to the SecureSync**

---

**Emailed general info from Paul Myers (3/5/12)**

➤ **In regards to HTTPS:**

- Certificates are used for HTTPS sessions. We only support the following.
- Loading x509 PEM certificates from the Web UI – Default for APACHE web server
- We support the user loading Public Keys via FTP by specific filename and then selecting then enabling that certificate for use using the WebUI
- This could be improved on with a better web UI but so far no one has complained or even used it I believe.
- We convert the following certificates from these types identified by file name to the x509 PEM used by Apache
- FTP a file named **cert.pem** which means **x509 PEM**
- FTP a file named **cert.der** which means **x509 DER**
- FTP a file named **certpem.p7c** which means **PKCS7 PEM**
- FTP a file named which means **PKCcdS7 DER**

**B) For an x509 PEM certificate (either copy/paste or upload the new certificate)**

1) **X509 PEM (plain text) certs can be simply copy/pasted into the web browser**

- Refer to the online SecureSync user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/UploadX509Cert.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/UploadX509Cert.htm)

**After extracting the certificate request via copy/paste, a new certificate can be created and then be transferred into the time server.**

**Email from Paul Myers (1 Nov 16)** I did issue a F5 refresh SOMETIMES and was forced to accept the new certificate in these case. BUT I did not have to login.

1. Using Chrome Login as spadmin (specify customer version)
  - i. Go to **Management->HTTPS Setup**
  - ii. Create a new HTTPS Self-Signed Certificate and Certificate Request
  - iii. Enter Certificate Request Parameters and select the checkbox at top of page
  - iv. Press submit
  - v. Select Certificate Request Tab and wait
  - vi. You will see "Creating new public/private keys, self-signed certificate and certificate request..."
  - vii. It takes TBD minutes depending on key length chosen to create new internal SELF-Signed certificate
  - viii. In the meantime, when the new Self-Signed certificate is created the Apache2 web server is restarted.
  - ix. If the user closes the tab OR hits F5 to refresh and watches the Certificate Request tab eventually the Certificate Request text will appear.
  - x. The user does not need to login to the web ui.
  - xi. The Certificate Request (CR) can now be provided to their CA Certificate Authority to create a Certificate they can reload it.

**2) X509 PEM (plain text) certs can alternatively be uploaded using the web browser**

- Refer to the online SecureSync User Manual:  
[:http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/LoadNonX509cert.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/LoadNonX509cert.htm)

**C) For formats other than PEM (such as DER and PKCS) (uploading a new certificate)**

- unless it is a X.509 PEM-format Certificate, once the HTTPS Certificate has been issued by your Certificate Authority, you have to upload the Certificate file to SecureSync,
  - Refer to online SecureSync User Manual:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/LoadNonX509cert.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/LoadNonX509cert.htm)

## Obtaining SSL Certificate details (such as expiration date) from SecureSync

- Refer to Salesforce Case 240116
- "View" the certificate in the web browser (Firefox, Internet Explorer, etc)

Q I am working on pulling the SSL Cert details for NTP devices. Do we have any API where we can pull SSL cert info like certname and Expiry date.

**A Reply from Dave L (27 July 2020)** Onboard the SecureSync we do not have a CLI command that will read the information you are looking for. Once installed the SSL Certificate expiration date and name cannot be read in the SecureSync. Openssl can be used to decode a certificate, but I am not sure the path to do this. Perhaps your web browser of choice can provide the information you need for the certificate.

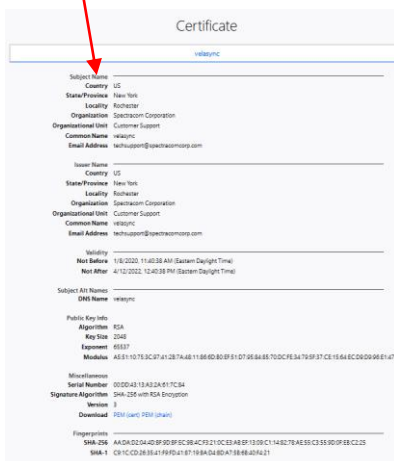
### Viewing certificate in Firefox:

1. Tools -> Options -> Privacy & Security -> View Certificate  
OR
2. Certificate can be viewed while establishing an HTTP connections



Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 10.10.162.20. The certificate is only valid for velasync.

Error code: MOZILLA\_PKIX\_ERROR\_SELF\_SIGNED\_CERT



---

## Desire to export private key or public/private key pair

- Refer to case 116919, Sep 2017 (for Cerner desiring to export private key for external storage)

**Per Paul Myers (26 Sep 17, as of at least v5.7.1 and below)** At this time we do not support access to the Public/Private Keys or allow their retrieval or loading on the SecureSync. The NetClock 9100/9200 I believe supported this feature, but we found it to be a security risk and NOT common practice to do this.

I think we would need to add web ui and some script changes to effect loading and retrieval of public/private keys and loading certificates. We would need affect changes for software update possibly and to add this change to a new release.

If we created a hotpatch to do this and allowed user access to add files it might teach them how to modify and attack our SecureSync security.

I think we need to do the following:

1. Discuss this with David Sohn and Ryan to see if we should do this.
2. Create a use case or user story as to WHY the customer must do this.
3. Determine if this results in an unacceptable security vulnerability?
4. Determine if any competitors allow this and is it a competitive advantage or disadvantage.

Possibly this might have to be NOT done, added as an expert mode or license hidden. I don't know yet.

<https://na28.salesforce.com/5001A00001Lt4DC>

---

## Backing-up of the HTTPS certificates

- As of at least versions 5.3.0 and below, public and private SSL certificates are not backed-up.

Q (from David Bradley) My question is, how to backup/save my private key. When requesting a purchased SSL certificate, you generate the private key and the certificate request pair. You then send the certificate request to the certificate provider.

If the spectracom NTP server is restored to factory conditions the SSL certificate is lost. If you were able to reinstate you previously generated private key you could simply re-use your SSL certificate, but without the private key you have generate a new key and request and contact the certificate provider for a replacement.

I cannot see any way within the web interface a way to copy the private key, I wondered if this was possible via the command line, using the SPADMIN user.

**A Reply from Morgan (9 Nov 15- applies to at least 5.3.0 and below)** We better understand your question now. From a Spectracom perspective we have not seem this as a problem, because the provider of our certificates allow us to regenerate a new certificate as long as we have active service with them. Will you certificate provider allow you to regenerate a new certificate during your activation period? If not let us know and I will forward to engineering.

---

## Issues with creating/installing a new SSL certificate (HTTPS certificate)

### A) Issues with creating a new certificate (specific to Chrome)

- (2 Nov 16) Dave L had a customer having issues with transferring in a new certificate using Chrome

**(Email from Dave L to Paul Myers)** Turns out Chrome was not updating the screens properly. We had much better luck using Firefox.

---

### B) Issues with creating a new certificate (specific to Internet Explorer- IE)

- Refer to Mantis case 1903 (noticed in version 4.8.7 Dec 2012)
- Internet Explorer 8 sometimes requires the user to press OK many times to accept the new HTTPS certificate. This ONLY observed with IE and does not always occur.

---

### C) Error message generated when creating a new certificate in version 5.3.1

- Refer to Mantis case 3202
- Error message asserted: “the item could not be saved. Please try again”.

**Email from Paul Myers (12 Jan 16)** If they really need this they might be able to drop to an old release, setup certificate then update and keep using it under new firmware. They just can't create a new one. ordan Comstock looked into it and has not found why yet.

---

### D) Creating a HTTPS Certificate Request and Public/Private key pair fails when entering FQDN (Fully qualified Domain Name, also known as Common Name) instead of entering the IP address (versions 5.1.7 and below. Fixed in 5.2.0).

- Refer to Mantis case 2940.
- Applicable to software versions 5.2.1 and below (fixed in update version 5.2.0 5.2.1 5.3.0)
- Common Name field won't accept a dot (and apparently not a hyphen either) unless it's for an IP address. But dots are needed to enter a common name (FQDN)
- Actually fixed in version 5.3.0 update (April 2015). Not sure what happened but a customer saw this issue with 5.2.0 installed and I also duplicated with 5.2.0 (30 Apr 15). So it looks like it really wasn't fixed in either 5.1.8 or 5.2.0 OR 5.2.1, 5.2.0 candidate was good, but the candidate was changed back, before 5.2.0 was released. Fix was also omitted from 5.2.1 update, as well.
- Note that a 'hyphen' now appears to be accepted in v5.3.0 (it appears in 5.3.0 and above, this field will now accept any character).

---

### E) Versions 4.8.5 and below have a web browser buffer size limitation

Q. I am able to create a valid CSR and self-signed certificate. Our CA accepts the CSR and issues a certificate. Uploading the certificate to the NTP server succeeds, regardless of the mechanism (HTTP or FTP). Validation of the certificate claims to succeed - but immediately afterward, the Apache web server process crashes and does not recover.

From /var/log/apache2/error\_log:

[Fri Apr 20 03:55:34 2012] [error] Init: Unable to read server certificate from file /etc/apache/ssl.crt/server.crt

[Fri Apr 20 03:55:34 2012] [error] SSL Library Error: 218529960 error:0D0680A8:asn1 encoding routines:ASN1\_CHECK\_TLEN:wrong tag

[Fri Apr 20 03:55:34 2012] [error] SSL Library Error: 218595386 error:0D07803A:asn1 encoding routines:ASN1\_ITEM\_EX\_D2I:nested asn1 error

- Refer to Salesforce Case Number 00005314 for specifics.

Likely cause is either inadvertently uploading the Certificate Request instead of the CA-generated Certificate (or not uploading a Certificate format we accept).

(5/18/12 KW) update to this issue. See comment below that the issue is due to the buffer size being limited to just 2kb. A file larger than this will be truncated. Paul Myers plans to increase buffer to 8k to likely prevent this from occurring again.

Refer to Salesforce case 5314 for details

**NOTE:** Versions 4.8.5 and below have a 2k web browser buffer size (should be increased to 8k in version 4.8.6). This can truncate an imported HTTPS certificate. If the certificate file is transferred with scp, this is not an issue.

Either transfer the file via SCP or update the SecureSync to a newer version of software.

**Email from Ian Roussos** It appears that the combination of the 4.8.5 software upgrade and SCP instead of HTTP upload has resolved my issue. I have a production certificate from the correct CA installed now.

When I used the HTTP upload process, the file size for /etc/apache/ssl.crt/server.crt did not change correctly – it was much  
pg. 566

smaller than it was supposed to be. When I used the SCP upload process the file size was exactly correct. This was true regardless of which CA I used. On 4.8.0, it did not appear to matter which transfer mechanism I used, the file did not update correctly.

Regardless, from my perspective this issue is closed. Thank you for your assistance and patience in helping me resolve it – I appreciate it.

---

### HTTP/HTTPS automatic re-direct

- The need to enter “HTTPS://” before the IP address: “HTTPS re-direct” can only occur if HTTP is enabled in Services (The redirect is inside the Spectracom box, so it has to be able to get in through http first).

With HTTP enabled, all you need to type in the browser window is the IP address (don’t have to type anything in front of the IP address. However, if the HTTP service is disabled in the spectracom box, you have to type “HTTPS://” in the browser (in front of the IP address) in order to be able to access the browser.

---

### Need to Reset HTTPS certificate (bad certificate was created, or certificate has expired, for examples)

**defcert** is the RS-232 command used to reset the HTTPS certificate (for security reasons, this command can only be performed via an RS-232 connection to the front panel SERIAL port. It’s not available with the other CLI interfaces, such as telnet and SSH).

- The only CLI command associated with certificates is the **defcert** command (to reset the certificate back to default)
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature Algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - An example “defcert” CLI syntax (5.6.0 and above only) is **defcert -sha256**
  - V5.6.0 also changed the default algorithm to **SHA256** for better security (the default in 5.5.1 and below was SHA1) .
  - As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access to IE8 and below

**Email from Keith (20 Jul KW)** One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can’t use this newer cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

The RS-232 command to reset the HTTPS Certificate back to the default value is “**defcert**”. This command is issued via the front panel RS-232 Serial port, using a PC running HyperTerminal (or other terminal emulator program). The PC’s com port should be connected to the NTP server using a standard DB9M to DB9F serial cable that is pinned straight-thru (at least pin 2 to 2, pin 3 to 3 and pin 5 to 5 for the minimum configuration). If a serial com port is not available on your PC, a standard USB to Serial adapter will be needed and its driver installed.

## “Account Locked due to **xx** failures”: Limit number of web browser/ssh login attempts/re-tries (entering incorrect password several times in a row)

- Refer also to the “User Accounts and Passwords” section further below for information.
- Refer also to Salesforce cases such as 172784
- Refer to “Number of Failed login attempts” in online SecureSync user guide: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/OpeningWebUI.htm?Highlight=logi n%20attempts](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/OpeningWebUI.htm?Highlight=logi n%20attempts)

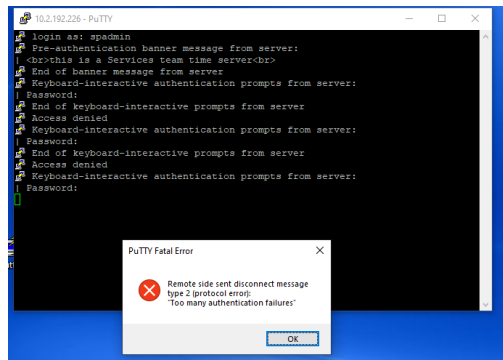
### Number of available login attempts before account is locked for 60 seconds (web browser versus telnet/ssh)

#### A) Web UI (HTTP/HTTPS)

- The number of failed login attempts for the Web UI (HTTP/HTTPS) is hard-set to (5) five failed login attempts, **with a 60 second lock thereafter**. This value is not configurable.
  - **Note from Keith (7 Sept 18)** The web browser doesn’t show/report any indication that it’s locked for 60 seconds after the 5<sup>th</sup> failed. The “lock” is only in the “background”.
- After waiting a full **60 seconds**, users are provided just **one** attempt thereafter to login successfully (instead of the normal five attempts) or the 60 second lock counter starts again (trying to login before 60 seconds has elapsed
- counts as that one attempt, and so user has to wait an additional 60 seconds before trying to login again).

#### Telnet/SSH:

- The number of failed login attempts for ssh is hard-set to **(3) three, with a 60 second lock thereafter**. This value is not user-configurable.



- After waiting a full **60 seconds**, users are provided just **one** attempt thereafter to login successfully (instead of the normal **three** attempts) or the 60 second lock counter starts again (trying to login before 60 seconds has elapsed counts as that **one** attempt, and so user has to wait an additional 60 seconds before trying to login again).

**Email from Morgan (11 Apr 16)** For all services we allow 5 login attempts then force a 60 sec lockout time then allow login attempts. This is to prevent bot's from rapidly attempting logins. This is not configurable.



---

## Associated config files

### A) httpd.conf file

- **Location:** /etc/apache2/conf
- **type** `cat httpd.conf`

### B) etc/apache/sites-enabled

- **type** `cat 000-httpd-default` (note: "000" is for the new browser, while "001" is for the classic interface browser)

- Refer to Salesforce Cases such as 116912 118079 and 218266 (excerpt below from 218266)

Q Can you provide instructions on how to regain access for a locked account?

ssh spadmin@kj05fd1i01

Password:

Account locked due to 38 failed logins

- MAY be related to using LDAP/Radius/Tacacs to connect to ssh, and the message is actually from their remote auth server (not from the SecureSync).
- Case 116457: we found SecureSync had a bad CF card.
- wtmp file may be full (reboot to delete)
- is browser still accessible?

**After talking with Stuart (12 Dec 2019)** after **three** failed SSH login attempts (or **Five** browser login failed attempts), a 60 second lock is asserted. Once this lock has been set, and after at least a full 60 second wait, users are given just one failed attempt (instead of the normal 3 for ssh, or 5 for browser) before another 60 second lock is placed again.

If another login attempt occurs before the full 60 second lock has elapsed, that allowed attempt is automatically failed, and so the user must wait at least another 60 seconds before attempting login again. After each failed login attempt, the failed login account counter is incremented.

He said this applies to both the SSH and web browser connections. So a failed ssh login with an account requires at least 60 seconds before using the same account to try logging into the browser.

In summary, if the wrong login password is initially issued three times (ssh) or five times (browser) make sure to wait at least 60 seconds before trying to login again, to prevent additional failed logins just due to trying to login too soon.

### Other example responses we've sent in the past for this message

**(Keith , Dec 2019 for 218266)** I've seen this error message asserted for a couple different reasons.

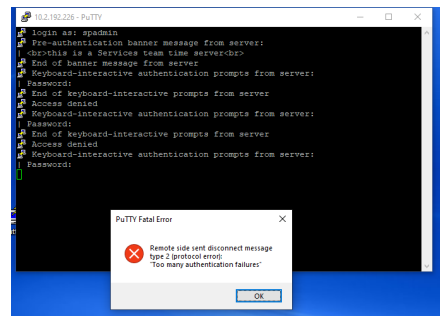
Question: Are you trying to connect to the SecureSync using an account on a remote authentication server (LDAP, Radius or TACACS)? Or, are you trying to connect directly to the SecureSync. using an account created inside the SecureSync (such as the default spadmin account, or a user account which has been created in the SecureSync)?

This message typically indicates an account on a remote auth server (LDAP, Radius or TACACS) has been locked out due to incorrect credentials. if you haven't already, try logging into the SecureSync using the spadmin account and the associated spadmin password.

If you are not logging in using an account on a LDAP/Radius/Tacacs remote auth server (if you are instead logging in directly to an account on the SecureSync) this is not a "normal condition" to occur for ssh in the SecureSync (SecureSync normally drops the attempted connection after just three failed password attempts, and without locking the account, as shown in the screenshot below). But a remote auth server may allow more than just three failed login, and then may lock that account after "some number" of failed attempts.

So, this condition would only occur in the SecureSync with direct login, due to abnormal operation of the SecureSync. We've

seen this condition previously caused once by the SecureSync needing to be rebooted (its wtmp directory was too full) and also once by the SecureSync's internal Compact Flash (CF) card starting to fail/needing to be replaced. Notice that rebooting a SecureSync having a CF card needing to be replaced can potentially prevent the SecureSync from being able to boot back-up thereafter, until its CF card has been replaced.



Are you able to login to the web browser, using the same credentials that were being used to try connecting via SSH?

If you are trying to connect to ssh using a remote auth server, the user account will likely need to be unlocked in that remote server. But if you are logging in directly with a SecureSync account, reboot/power cycle the SecureSync and then try connecting again.

Please let us know this info helped you connect to the SecureSync! Thanks in advance!

**(Dave L, Sept 2017 for 116457)** This oz00pdm11 Unit was replaced just two months ago so it is very new. There could be issues with the configuration like the DNS Server addresses were not entered or there are user accounts that need to be setup. It indicates the password you are using is incorrect. Please note the password is case sensitive. Can you login as spadmin using the default password admin123?

**(Dave L, Aug 2017 for 116457)** Is the web UI accessible? This problem may be caused by a wtmp file becoming full. A reboot should fix the problem. Can you try a reboot and send the results?

**(Morgan, April 2018 for 160169)** Are you trying to login in with the default account information (spadmin/admin123)? Did you give it 90 min. and try to login again? What happens if you do the "resetpw" command from the keypad? Let me know what happens.

---

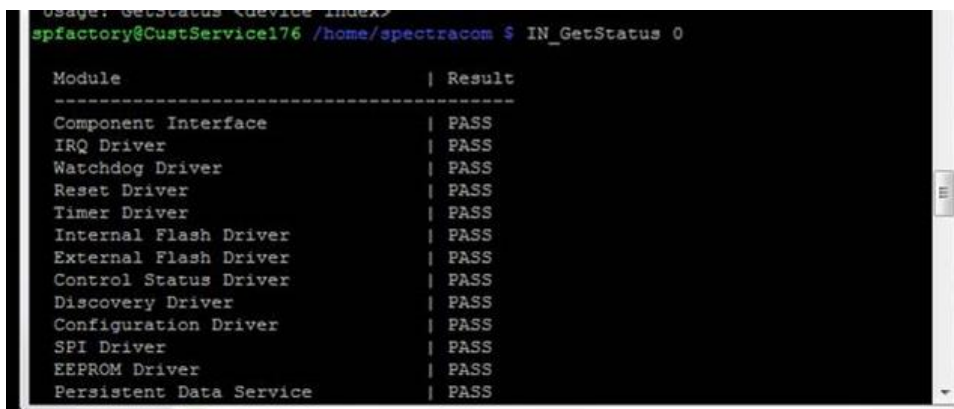
## \*\*Apache Web browser/general lock-up troubleshooting (error messages displayed/abnormal web browser operation, sluggish browser, etc)

- Good document for troubleshooting web browser/ssh issues:  
<https://www.linode.com/docs/troubleshooting/troubleshooting/>

## \*\*Indications of KTS (Kramden Timing System) not running

- Front panel LED time display frozen (not incrementing)
- Potentially- Several “KTS failed to read” log entries in the logs
- Potentially- difficulty with communicating with the browser/CLI due to ETX not being able to talk to KTS.

**Note:** Refer to the **IN\_GetStatus 0** CLI command in the CLI section of this document to display a list of pass/fail state for KTS initialization (Example below). See if any items report FAIL. This command is available in the spadadmin account.



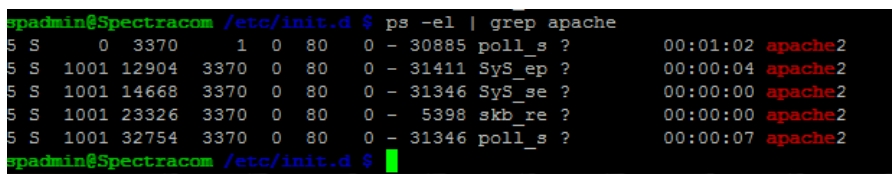
```
Usage: getstatus <device index>
spadfactory@CustService176 /home/spectracom $ IN_GetStatus 0

Module | Result
-----|-----
Component Interface | PASS
IRQ Driver | PASS
Watchdog Driver | PASS
Reset Driver | PASS
Timer Driver | PASS
Internal Flash Driver | PASS
External Flash Driver | PASS
Control Status Driver | PASS
Discovery Driver | PASS
Configuration Driver | PASS
SPI Driver | PASS
EEPROM Driver | PASS
Persistent Data Service | PASS
```

---

## Verifying if Apache web browser is actually running

- To see if Apache is running, type **ps -el | grep apache** <enter> (where it will list everything with the name typed after “grep”):



```
spadadmin@Spectracom /etc/init.d $ ps -el | grep apache
5 S    0  3370      1  0  80    0 - 30885 poll_s ?        00:01:02 apache2
5 S   1001 12904  3370  0  80    0 - 31411 SyS_ep ?        00:00:04 apache2
5 S   1001 14668  3370  0  80    0 - 31346 SyS_se ?        00:00:00 apache2
5 S   1001 23326  3370  0  80    0 - 5398  skb_re ?        00:00:00 apache2
5 S   1001 32754  3370  0  80    0 - 31346 poll_s ?        00:00:07 apache2
spadadmin@Spectracom /etc/init.d $
```

---

## \*\*\*REST API interface/Postman (alternate to using the standard web browser or CLI)

- Requires 1200 SecureSync software **versions 5.4.5** or above be installed.
- Allows for status and configuration data to be sent and retrieved without having to use the Web UI.
- The REST API utilizes JSON (JavaScript Object Notation) formatted data for sending commands and receiving status information from the devices (performing HTTP GET and POST operation)

Links to references/additional info on REST API

- REST API /Postman collection on our website: REST API /Postman collection on our website: <https://www.orialia.com/document/secsync-netclock-9400-rest-api-collection-and-documentation/>
- Ron Dries' Blog about REST API (on our site): <https://www.orialia.com/resources/blog/ron-dries/2018/rest-api-powerful-interface-remote-control-pnt-deviceshttps://files.spectracom.com/client-downloads/5690>
- Refer also to documents (such as API guide) in: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\REST API - Postman and Python scripts>
- Refer to tutorial sites such as <https://restfulapi.net/> and <https://restfulapi.net/rest-api-design-tutorial-with-example/>  
For the general (non-product specific info applying to all products compatible with REST API) REST API info, refer to "**REST API interface/Postman**" section in the custassist doc: <..\CustomerServiceAssistance.pdf>

## REST API/Postman documentation

- Here is a link to what we have for the REST API documentation in SecureSync. <https://www.orialia.com/document/secsync-netclock-9400-rest-api-collection-and-documentation/>
- For more info, refer to "**REST API/Postman documentation**" in <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>

## Availability/support of the REST API (Software version-specific info)

- 1200 SecureSyncs: available with at least versions 5.4.5 and above (possibly also earlier than version 5.4.5)  
**Update to Dave Sohn's note below (14 Nov 16, v5.4.5 is current version)** not sure when this was added/made available. But I believe Ron Dries has been using this lately to write custom python scripts.  
~~Email from Dave Sohn (9 Apr 2014) The secure REST API is part of our roadmaps. I don't think we have any dates for this feature though.~~

## "403 Forbidden" errors / Report of login to REST API broken after 5.9.1 to 5.9.2 update

- 403 Forbidden error when connecting with HTTPS, but not with HTTP
  - No or invalid SSL certificate loaded into Postman (**Gear** icon at top of page -> **Settings** -> **Certificates** tab)
- Refer to Salesforce Cases such as:
  - 265557: Can login in-house but not outside through the VPN. a **403 Forbidden** error was encountered while trying to use an ErrorDocument to handle the request. Apache Server at xxxxxxx.local Port 44
  - 271534 (Aug 2021- Excerpt below)  
**Summary:** Per Ron Dries, v5.9.2 (and above) modified REST API to be more like 2400 SecureSyncs. A "Mod" in REST API is required to support.

"We interface to our time servers using the SecureSync REST API, and our method for logging in no longer works with SW version 5.9.2. We POST "Login" requests to [IPAddress]/users/login.json with the username and password, but this stopped working when we upgraded a unit from 5.9.1 to 5.9.2. As a test, we have used the Postman app and tried the Login request that was provided in SecureSync\_REST\_API.postman\_collection.json. It works correctly to login to a server with SW 5.9.1 or earlier, but when we try the login request to a server with version 5.9.2, it fails. The response shown in the Postman app indicates "This application requires JavaScript. Your current browser or settings are not supported."

Since the login fails, every subsequent request for status information gets "**403 Forbidden**" response and our software has no way to monitor status. Is there a new/alternate method for logging in via the SecureSync REST API? Or can this issue be fixed in the next version of SW?"

Answer/Reply below from Ron Dries (18 Aug KW)

Hi Keith,

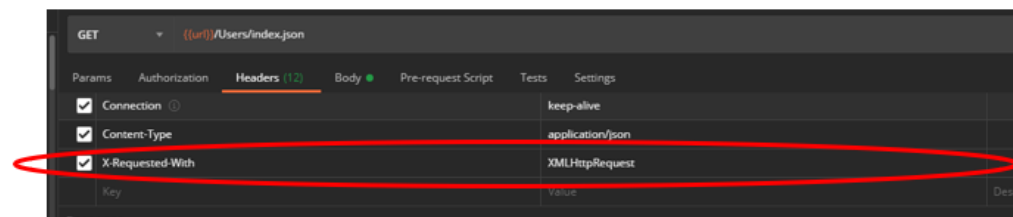
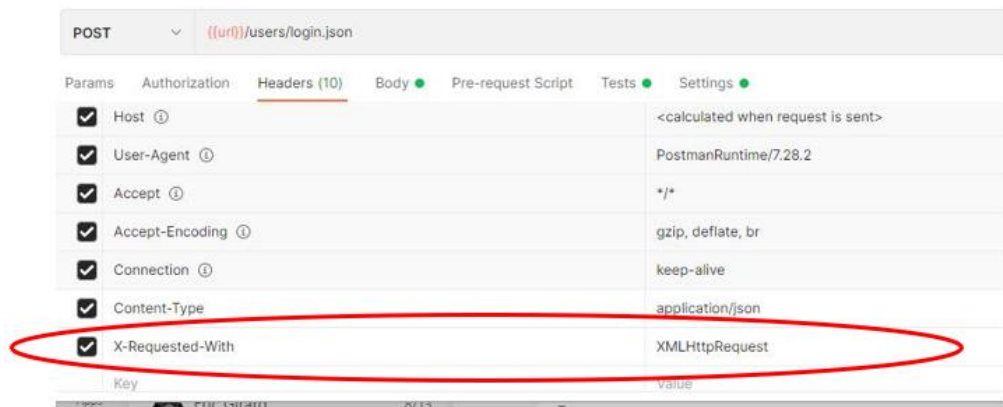
I believe they have made a change in the REST API to match the SecureSync 2400.

A new header value is now required in the requests.

The key value pair is:

### **X-Requested-With: XMLHttpRequest**

In postman it can be added like the below example:



A Python Request example would be:

```
import requests
import json

url = "10.10.162.244/users/login.json"

payload = json.dumps({
    "User": {
        "username": "spadmin",
        "password": "admin123"
    }
})
headers = {
    'Content-Type': 'application/json',
    'X-Requested-With': 'XMLHttpRequest'
}
```

```
response = requests.request("POST", url, headers=headers, data=payload, allow_redirects=False)

print(response.text)
```

---

## General info about REST API

The graphical Web User Interface ("Web UI") used with Spectracom's SecureSync and NetClock time servers has a built-in REST API which allows for status and configuration data to be sent and retrieved from the device without having to use the Web UI. This is useful for machine-to-machine communication, as well as for developing mobile apps. The REST API uses the JSON data format when performing HTTP GET and POST operations.

To perform these HTTP operations, it is necessary to know the data format required to retrieve and send data to SecureSync. Spectracom's **Postman**<sup>™</sup>1 collection is a compilation of frequently used operations which may serve as examples of how to pull and send data through the SecureSync API.

**Note:** refer to "**Postman details**" further below

- Refer also to tutorial sites such as <https://restfulapi.net/> In simplest words, in the REST architectural style, data and functionality are considered resources and are accessed using **Uniform Resource Identifiers (URIs)**. The resources are acted upon by using a set of simple, well-defined operations. The clients and servers exchange representations of resources by using a standardized interface and protocol – typically HTTP.

Resources are decoupled from their representation so that their content can be accessed in a variety of formats, such as HTML, XML, plain text, PDF, JPEG, JSON, and others. Metadata about the resource is available and used, for example, to control caching, detect transmission errors, negotiate the appropriate representation format, and perform authentication or access control. And most importantly, every interaction with a resource is stateless.

All these principles help RESTful applications to be simple, lightweight, and fast.

References:

<http://roy.gbiv.com/untangled/2008/rest-apis-must-be-hypertext-driven>

[http://www.ics.uci.edu/~fielding/pubs/dissertation/rest\\_arch\\_style.htm](http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm)

- and <https://restfulapi.net/rest-api-design-tutorial-with-example/>

## Resource URIs/endpoints

- These **resource URIs are endpoints for RESTful services**.

---

## Postman details

- For more info, refer to "**Postman details**" in <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>

## About Postman

Postman is an HTTP client that serves as a development app to prototype and test APIs. As of December 2016, the Postman app is available for Google Chrome<sup>™</sup>, or as native apps for Microsoft Windows<sup>™</sup>, Mac OS X or later, and Linux: <https://www.getpostman.com/apps>.

Postman can be used to send the requests to a SecureSync or NetClock unit, and it will return the JSON response from the device. The JSON response is formatted in a clean and legible format that is useful for understanding each of the API calls. This allows to quickly test API calls without having to develop test software, and the format of the data returned can be easily analyzed for inclusion into scripts or applications that can consume the data.

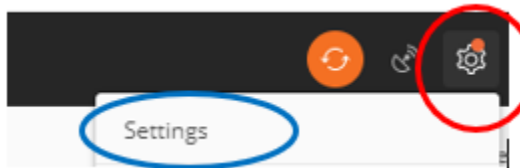
## Downloading and Installing the Postman<sup>™</sup> Chrome<sup>™</sup> App

1. Install the Google Chrome web browser.
  2. Navigate to <https://www.getpostman.com/apps>, and select "Download Postman for Chrome".
  3. The Chrome Web Store will open, displaying the Postman app download window. Click ADD TO CHROME.
  4. Once the Chrome App Launcher has opened, click the Postman app icon to open Postman.
  5. Create an account by signing up. This will ensure your requests, collections, environments and history data are saved for future reference.
- 6. The app will open.**

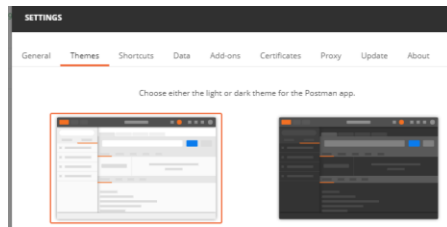
## Familiarizing Yourself with Postman

### Optionally toggle between White or Black background

1. Select the Settings (Gear ICON) drop-down in upper-right corner. Click **"Settings"**

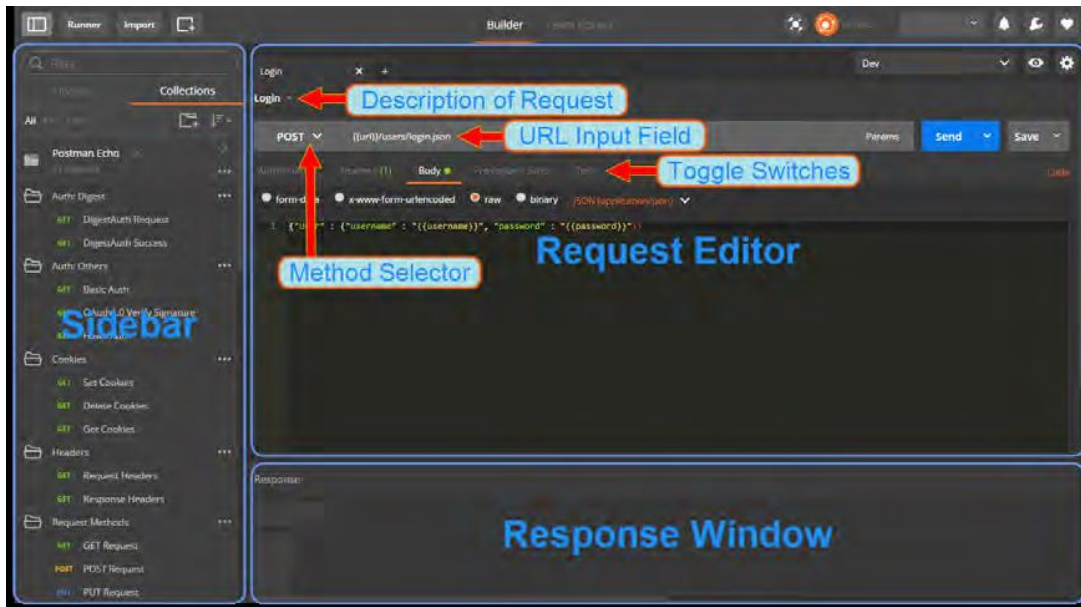


2. Select **"Themes"** and then click either the White or Black background



The following is a brief overview of the Postman UI. More comprehensive assistance can be found under <https://www.getpostman.com/docs>.

The Sidebar lists the requests stored in the loaded Collections (see "Spectracom REST API Developer Guide" on the previous page), and – under the History tab – a list of recently submitted requests.



The Sidebar lists the requests stored in the loaded Collections (see "Spectracom REST API Developer Guide" on the previous page), and – under the History tab – a list of recently submitted requests.

### Postman functionality highlights:

Create requests by conveniently specifying Method, URL parameters, Header and Body. Submit API calls quickly to test scripts; generate code snippets that can be copied and pasted.

Specify authorization to be used.

Display responses in different formats e.g., "pretty", "raw", or as rendered HTML pages.

Organize and store requests in Collections.

Store request parameters that will be used repeatedly (e.g., keys and values used as login credentials) in development project-specific Environments.

Access history of sent requests.

Capture documentation for requests in a description field.

## Importing the Spectracom Collection

Spectracom's Postman™ collection provides examples of how to pull and send data through the API.

To import this collection:

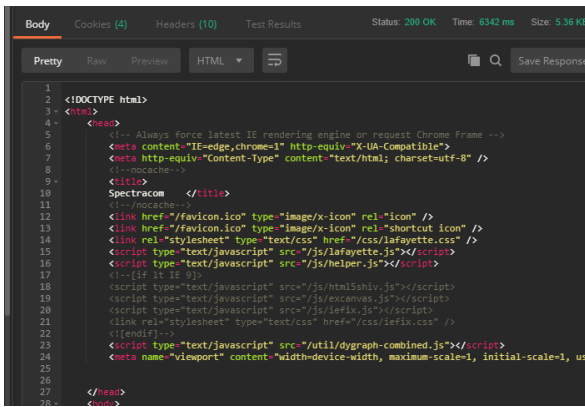
1. Unzip the Spectracom REST API kit to a local directory of your choice.
2. Unzip the kit files to a local directory of your choice.
3. Open the Postman app, using the credentials of your previously created account.
4. Import the SecureSync REST API Collection:
  - a. With the Google Chrome app, click the Import button at the top left corner of the screen. For the standalone app, click the Collection menu option on the top of the screen, then select Import.

➤ Navigate to Collections > Import: Choose File.



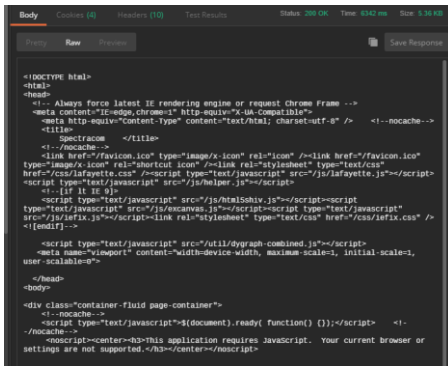


## Pretty tab



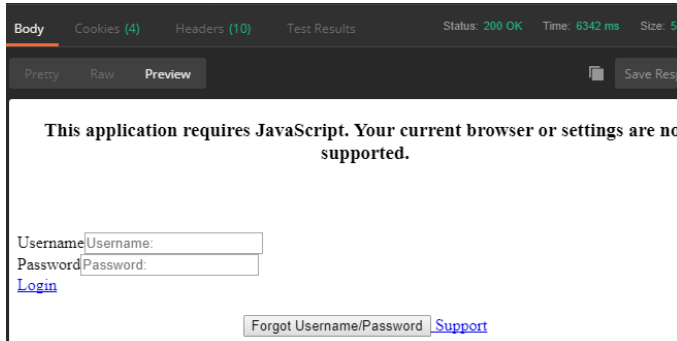
```
1
2 <!DOCTYPE html>
3 <html>
4   <head>
5     <!-- Always force latest IE rendering engine or request Chrome Frame -->
6     <meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
7     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
8     <!--no-cache-->
9     <title>
10    Spectracom </title>
11    <!--no-cache-->
12    <link href="/favicon.ico" type="image/x-icon" rel="icon" />
13    <link href="/favicon.ico" type="image/x-icon" rel="shortcut icon" />
14    <link rel="stylesheet" type="text/css" href="/css/lafayette.css" />
15    <script type="text/javascript" src="/js/lafayette.js"></script>
16    <script type="text/javascript" src="/js/helper.js"></script>
17    <!--if lt IE 9>
18    <script type="text/javascript" src="/js/html5shiv.js"></script>
19    <script type="text/javascript" src="/js/excanvas.js"></script>
20    <script type="text/javascript" src="/js/ie10.js"></script>
21    <link rel="stylesheet" type="text/css" href="/css/iefix.css" />
22    <![endif]-->
23    <script type="text/javascript" src="/util/dygraph-combined.js"></script>
24    <meta name="viewport" content="width=device-width, maximum-scale=1, initial-scale=1, us
25
26  </head>
27  <body>
```

## Raw tab



```
<!DOCTYPE html>
<html>
<head>
<!-- Always force latest IE rendering engine or request Chrome Frame -->
<meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <!--no-cache-->
<title>
Spectracom </title>
<!--no-cache-->
<link href="/favicon.ico" type="image/x-icon" rel="icon" /><link href="/favicon.ico"
type="image/x-icon" rel="shortcut icon" /><link rel="stylesheet" type="text/css"
href="/css/lafayette.css" /><script type="text/javascript" src="/js/lafayette.js"></script>
<script type="text/javascript" src="/js/helper.js"></script>
<!--if lt IE 9>
<script type="text/javascript" src="/js/html5shiv.js"></script><script
type="text/javascript" src="/js/excanvas.js"></script><script type="text/javascript"
src="/js/ie10.js"></script><link rel="stylesheet" type="text/css" href="/css/iefix.css" />
<![endif]-->
<script type="text/javascript" src="/util/dygraph-combined.js"></script>
<meta name="viewport" content="width=device-width, maximum-scale=1, initial-scale=1,
user-scalable=no">
</head>
<body>
<div class="Container-Fluid page-container">
<!--no-cache-->
<script type="text/javascript">(document).ready(function() {})</script> <!--
--no-cache-->
<script><center><h3>this application requires JavaScript. Your current browser or
settings are not supported.</h3></center></script>
```

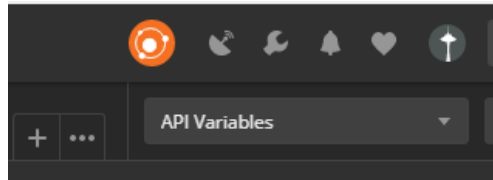
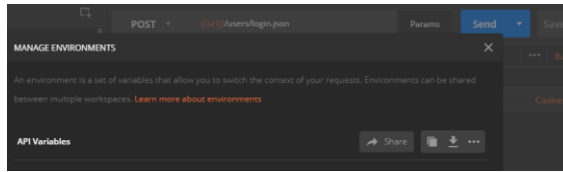
## Preview tab



- **GET:** Whenever a user **accesses a page**, the View component issues a **GET** request to the Controller, since the user ultimately wants to retrieve (or: GET) the data that is displayed on the loaded page.
- **SET/POST:** If, however, a user wants to **add or configure** a setting, the View component will issue a **SET** (or: **POST**) request to the Controller. In both cases, the Controller will receive the request, decide which operation to apply (CRUD), and then forwards the processed request to the Model, which will execute the request.

➤ Refer to “**Spectracom REST API Developer Guide**” (included in zip file and at: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts](#))

1. Open Postman installed on desktop of PC
2. “**Import the DEV environment**” Click the gear icon in upper-right corner, click **import** and select the file “**API Variables.postman\_environment.json**” file. “**API Variables**” will be displayed in the middle and top-right side of the page (as shown below).

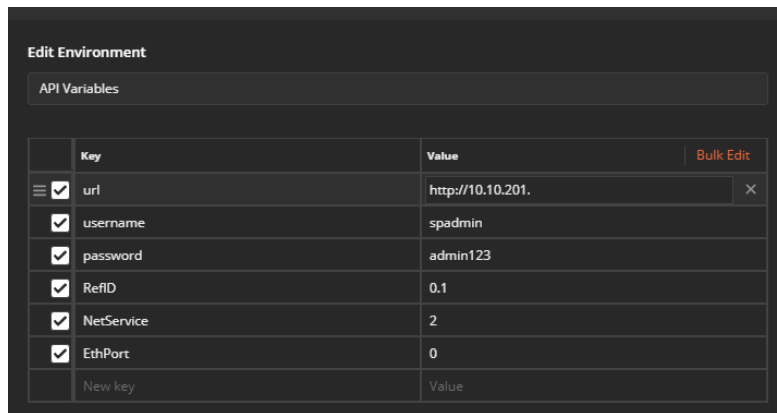


3. In the **Manage Environment** drop-down menu (next to the EYE button), select **Dev** to load the environment imported above.

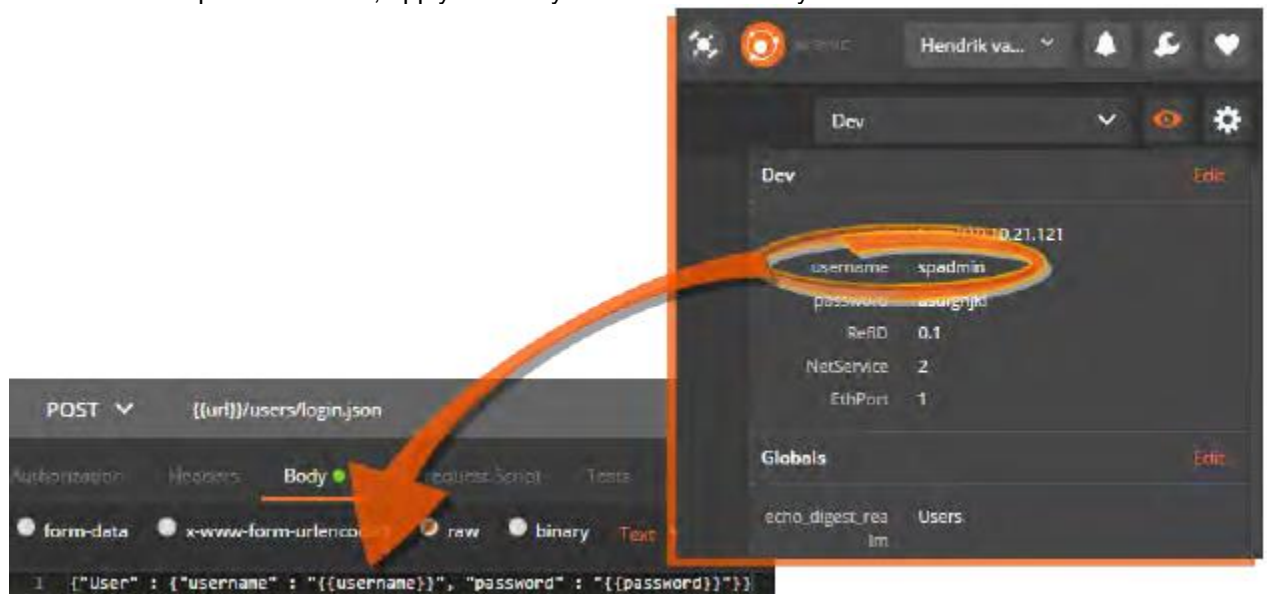
### API Variables window (url, account login info)

4. Click the **EYE** button to see which environment variables have been loaded with this environment file: One variable is called **url**, another one is **spadmin**, etc.

Click edit to change any/all the values (such as the URL of the desired SecureSync). Then click **“Update”**.



To use a development variable, apply two curly brackets in the body code:



To test, click the blue **Send** button (top-right corner of the page). The coding window will display the requested code:

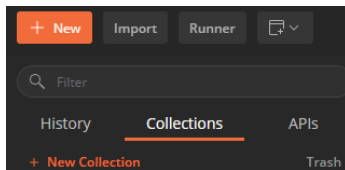
```

Body
2010K 2294 ms
Prevy
JSON
1 {
2   "url": {},
3   "data": "quis possure augue vel cursus pharetra. In luctus a ex nec pretium. Praesent neque quam, tincidunt nec leo eget, rutrum vehicula magna.\)Mecenas consequat elementum elit, id semper sem tristique et. Integer pulvinar enim
4   quis consectetur interdum volutpat.",
5   "files": {},
6   "meta": {},
7   "headers": {
8     "host": "echo.getpostman.com",
9     "content-length": "255",
10    "accept": "*/*",
11    "accept-encoding": "gzip, deflate, br",
12    "accept-language": "en-US,en;q=0.8,de;q=0.6",
13    "cache-control": "no-cache",
14    "content-type": "text/plain",
15    "origin": "chrome-extension://fhqjpkifljhgagmehobnciddomy",
16    "postman-token": "c1141466-3d4e-6928-63d2-403721245480",
17    "user-agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.67 Safari/537.36",
18    "x-forwarded-proto": "https"
19  },
20   "time": null,
21   "url": "https://echo.getpostman.com/post"
22 }

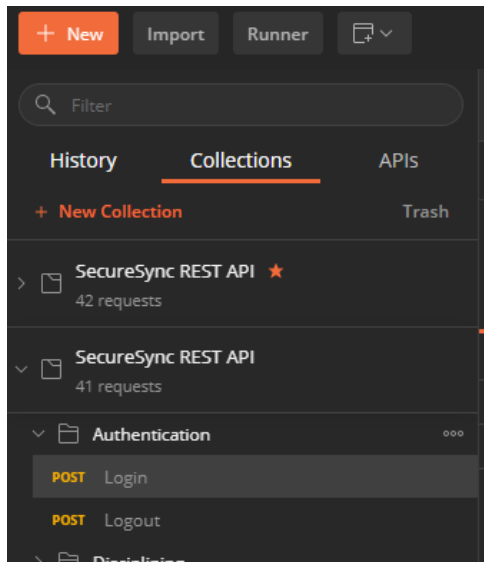
```

## Login to the time server to perform Get/Post commands

1. On the left-side of the page, select the **Collections** tab



2. Expand **“SecureSync REST API”**, and perform **Authentication** -> **“Login”** to the desired SecureSync (highlight **“Login”** and press the **Send** button (in blue))



3. Scroll down about 56 lines and verify it indicates (in white text) **“Welcome, spadmin</spa”**

```

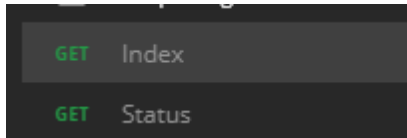
56 <span class="username">Welcome, spadmin</span><a href="/Users/logout"

```

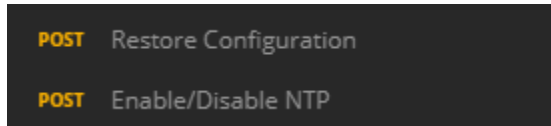
- This confirms you are logged into the time server. No need to login again for each task desired to be performed

## Performing Gets/Posts commands, once logged in:

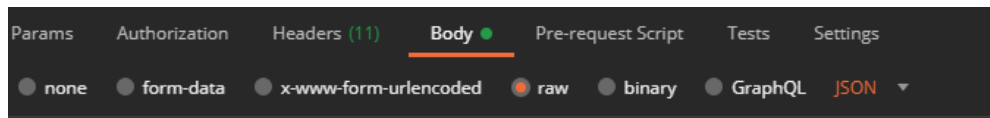
- For “**Get**” (in green) commands (cannot edit Get commands), select the “**Body**” tab in the second main window down



- For “**Post**” (in yellow) commands (which allows edits of the values)



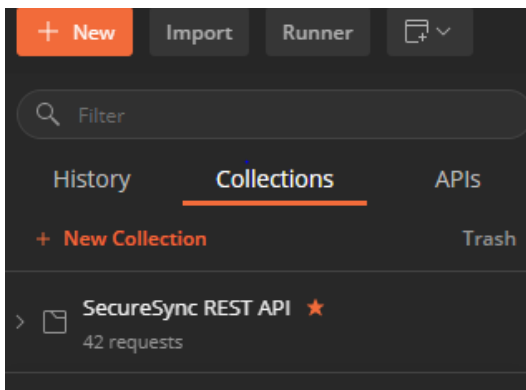
1. Select the “**Body**” tab and select “**JSON**” in the drop-down.



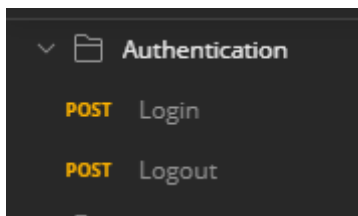
2. Then select “**raw**” on the upper window to edit values (in yellow text).

## Logout of the the time server (when done)

3. On the left-side of the page expand “**SecureSync REST API**”,



4. Expand and perform **Authentication** -> “**Logout**” to the desired SecureSync



## Other available commands not included in the default Dev package

GNSS receiver status

Find out what web browser (and its version) they are using on the PC (such as IE11, Firefox,

etc).

- **IE 11 and above** require a valid HTTPS certificate (doesn't allow you to accept an invalid certificate to proceed)

Per: [https://answers.microsoft.com/en-us/windows/forum/windows\\_7-update/after-applying-3205394-ie11-version-is-listed-as/4a1dc892-8bcb-45f0-9390-418c81d753db?page=2](https://answers.microsoft.com/en-us/windows/forum/windows_7-update/after-applying-3205394-ie11-version-is-listed-as/4a1dc892-8bcb-45f0-9390-418c81d753db?page=2)

My IE 11 lost ability to "Continue on..." when there is a certificate error. That option is usually between the "We recommend you close this page" and the "More information" line

---

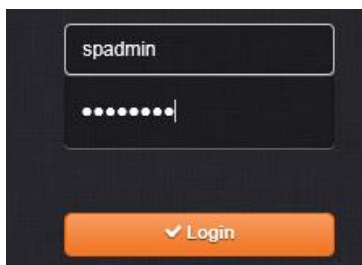
### A) Issue observed here (Jan 2018): “TLS handshake”taking too long in Mozilla Firefox” (not able to access login page)

- I was able to access one of our SecureSyncs via HTTPS, but not able to get to login page of two others (I was able to reach all units via SSH and also HTTP, but not with HTTPS)
- “TLS Handshake” was reported at bottom of browser page for several seconds when trying to access the other two units
- Also noticed that FireFox was not prompting me to accept a self-sign),
- Fix (excerpted and modified in red, below) was to rename the file, to have a new file be generated, and then restart Firefox
- Refer to <http://talk.manageiq.org/t/solved-firefox-performing-a-tls-handshake-is-slow/3046/4>
- I had similar issues. <https://www.thessslstore.com/blog/troubleshoot-firefoxs-tls-handshake-message/> 3.0k suggested a fix which worked for me
- An easy way to do this is to browse to about:support and then click the Open Folder button for the Profile Folder. Locate cert8.db (and cert9.db) in your file explorer and rename the file (e.g. “cert8.db.bak”/ “cert9.db.bak”) so that Firefox replaces it. Restart the browser and try visiting an affected site again. If the page loads normally, **you have confirmed the issue is related to the local certificate database storing too many self-signed certificates with the same name.**

---

### B) Can't login to JUST the newer black/charcoal browser (no error message displayed, and username keeps disappearing with each login attempt). But if invalid credentials are entered, it indicates “invalid username or password”

- CLI login is fine, and CAN login to the classic browser using HTTPS.



### C) Entering valid login credentials and then after pressing login (username field goes blanks)”



1) When logging in using “HTTPS” make sure HTTPS is enabled in Services (cli command **servget 6** <enter> should respond HTTPS is enabled

- If HTTPS is disabled, type: **servset 6 on** <enter>

2) This issue most likely due to “Cookies” being “blocked” or “disabled”

- This condition will cause a certificate error to occur
- This condition is also discussed further below in this list of possible issues (CERTIFICATE ERRORS)

Haven't run across this one in a VERY long time. But its an even simpler explanation and also matches what you are observing. I just duplicated it with my IE11.

In IE, go to **Tools -> Internet Options**. Select the **Privacy** tab, and press **Advanced**

The **Advanced Privacy Settings** window which opens, make sure both the **First party** and **Third party** cookies are not “**blocked**”. If I recall correctly, I think it's only the first party cookies which matter (but configure them both the same, just in case). If the cookies are blocked, you won't be able to login, there won't be an error message displayed, and the username goes away each time.



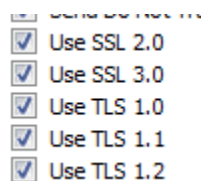
Or, if you select “**prompt**”, but then don't allow the cookie requests while actually logging in, the same effect happens- there is no error message displayed and the username disappears each time.

3) Could also potentially be due to the HTTPS certificate failing due to an incorrect “Common Name” (“Spectracom”) in our default HTTPS certicate (need to change this value to the applicabe hostname or static IP Adres they use to login to the browser).

- IE Versions 10 and below (as well as IE 11, before v11.9600) allow a user to still accept an invalid certificate. IE 11.9600 and above (IE 11.0.49 does not exhibit this, but 11.9600 does) do not allow the ability to accept an invalid certificate (such as the default factory certificate) Refer to: <https://blogs.msdn.microsoft.com/ieinternals/2013/12/12/continue-link-missing-from-certificate-error-page/>.

4) SSL/TLS selection

- In IE, go to **Tools -> Internet Options**. Select the **Advanced** tab. Scroll down towards the bottom



- If **HISEC** (the “**Enable High Security**” checkbox) is enabled in the time server, make sure “**TLS 1.2**” is enabled.

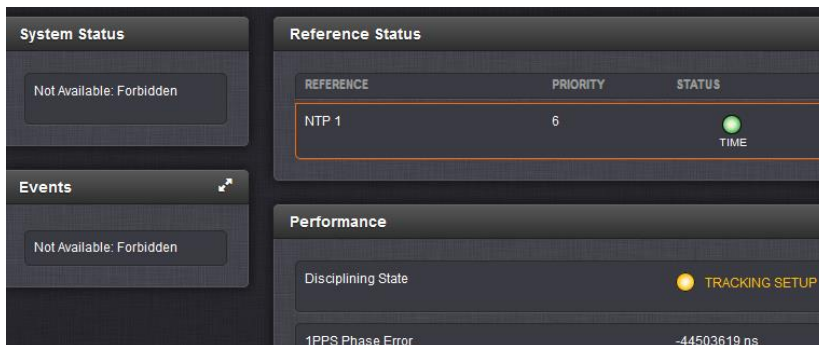
- the “**Enable High Security**” checkbox: is in the *Management* -> *Network Setup* page of the browser (press the “**web interface settings**” button on the left). Then select the “**Enable High Security**” checkbox in the “**Security Level**” tab (as shown below):



**D) Error message of “Not Available: Forbidden” error message displayed in newer web browser only (classic interface login is fine) after updating to version 5.3.1**

**Symptom:** “*Not Available: Forbidden*” error message is being displayed while trying to login to the newer (black/charcoal) web browser (login fails with “*Not Available: Forbidden*” displayed). But can still successfully login to the classic interface browser.

**This message indicates not currently logged into the browser (earlier login may have since timed-out)**



**Fix:** refresh the browser page and login.

This issue is due to updating to software version 5.3.1, when a save configuration file has ever been previously created. The fix to this is to just reboot the unit once (reboot CLI command, reboot from classic interface or power cycle)

Note this message of “Forbidden” can also indicate network access restriction has been configured. Try typing the CLI command of **unrestrict** if a reboot/power cycle does not restore access to the newer browser (with the error message no longer displayed).

**E) Error code: **ssl\_error\_no\_cypher\_overlap** displayed when trying to connect.**

- Verify the browser (IE, Firefox, Chrome) on the PC is up to date

**Email from Harris (3 March 15):** Brian, I loaded the 5.2.0 software and now my Firefox browser won't connect to the webpage. My firefox version is 13.0.1. the page message is:

Secure Connection Failed

An error occurred during a connection to 10.128.13.97.



Cannot communicate securely with peer: **no common encryption algorithm(s)**.

(Error code: ssl\_error\_no\_cypher\_overlap)

The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.

Please contact the website owners to inform them of this problem. Alternatively, use the command found in the help menu to report this broken site.

**Keith's finding:** Firefox 13 was release in 2013. I recommended updating Firefox to a much newer version.

## F) Apache Web browser no longer accessible (can't even get to login prompt), but ping, telnet, SSH still work

### 1) Versions 4.8.9 and below (ssh may or may not be accessible)

- Refer to memory leak issue (**free -m** CLI command response needs to be above about 100MB to be able to open/run Apache)

### 2) Versions 5.0.0 and above

- "Connection refused" may be displayed
- CF card may be full, especially in versions such as 5.0.2 for instance, due to nullmailer (nullmailer fixed in 5.1.2)
- Perform a **df -h** CLI command to check disk usage.

```
spadmin@spectracom ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M  53% /
/dev/hdal       963M  480M  434M  53% /
devtmpfs       248M   0  248M   0% /dev
```

- Can't delete logs in earlier versions such as with v5.0.2, but deleting any update files that may be present and also running the cleaner patch (uploading the cleaner file via FTP upload of the cleaner file and then using the **sysupgrade cli** command) may help.

**Email Keith sent to Mark Day (1 Apr 15 for his customer JPMC.** We have reviewed the SecureSync logs that you provided us with. Based on these logs entries and also due to the CLI interface operating normally, we suspect this condition you are observing with the web browser not connecting is related to either the unit's configuration or the Apache web browser.

The logs don't show an immediate indication of why you aren't able to connect to the web browser. We would like to request from you a copy of the SecureSync's configuration files, if possible, to correlate with the logs. And if it is feasible, our engineers being able to remotely connect to the SecureSync (or being able to "remote desktop" into a PC on the same network) would also likely be very helpful. However, if this isn't possible for security reasons, we completely understand.

Can you perform a few steps for us that will likely help with the diagnosis of this condition?

## G) Invalid / undesired IP address or subnet value may have been entered in the Access Control table

- Try performing an **unrestrict** <enter> cli command

**Note:** as of at least v5.4.5, this command not available via the front panel)

## H) With an FTP connection to the SecureSync:

- The unit's config files are located in the /home/spectracom/config directory. Can you FTP and bundle these config files into a single bundle file and then send them to us?

**Note:** the log bundle (starting in v5.2.1 I believe) now includes Apache logs which may be helpful.

I) With a telnet or ssh connection to the SecureSync:

1.Type **rc-status** <enter> and send us a screenshot of the response. (**rc-status | grep apache**)

Note: look to see if any services are unexpectedly “crashed” or stopped

```
spfactory@Spectracom /home/spectracom/log/ntpstats $ rc-status | grep apache2
apache2-cert [ started ]
apache2 [ started ]
spfactory@Spectracom /home/spectracom/log/ntpstats $
```

2.Type **ps -elf**<enter> and send us a screenshot of the response. (**ps -el | grep apache**)

3.Type **df -h** <enter> and send us a screenshot of the response

Note: CF card usage is now reported in the browser (alleviating need to have to use CLI command)

Note: Update version 5.2.0 added CF card memory status to the newer web browser (not available in classic interface). Note: Also added ability to delete logs and Statistics from the same location

Tools -> Upgrade/Backup page of the browser (under “Disk Status”)



4. Type **servget 6** <enter>. Verify the response indicates **HTTPS Service** is **Enabled**
5. Type **servget 5** <enter>. See if the response indicates **HTTP Service** is Enabled or Disabled.
6. If **servget 5** (referenced in the step above) indicated **HTTP** is currently **Disabled**, type **servset 5 on** <enter> to enable HTTP.
7. Type **servset 6 off** <enter> to disable HTTPS.
8. Try connecting to the web browser with “**HTTP://**” in front of the address (instead of using “https”)
9. Type **servset 6 on** <enter> to enable HTTPS.
10. Try logging into the browser with “**HTTPS://**” in front of the address.
11. Type **unrestrict** <enter> to clear the network access restriction table (may have inadvertently entered a value in this table that locked out the address of the PC, the subnet or all network IP addresses).
12. Try logging into the browser again with “**HTTPS://**” in front of the address.
13. Type **defcert** <enter> to reset the HTTPS certificate (note there won’t be a response to this command).
  - The only CLI command associated with certificates is the **defcert** command (to reset the certificate back to default)
14. Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - Example syntax is **defcert -sha256**

15. V5.6.0 also changed the default algorithm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).
16. Try logging into the browser again with “**HTTPS://**” in front of the address.

#### J) Neither Apache or telnet/ssh now available.

- See if can connect via RS-232 Serial port on the front of the unit.
- Try connecting to browser/telnet again after rebooting
  - If it can connect after power cycling, get both the log and config bundles to review. Check the kern log and System log. See if there are any “out of memory” entries in the System log. (Refer to the System.log for more info on this condition)

#### K) HTTPS certificate somehow corrupt

- Try performing a **defcert** <enter> cli command (as of at least v5.3.0, this command not available via the front panel)
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - Example syntax is **defcert -sha256**
  - V5.6.0 also changed the default algorithm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).

#### L) Memory leak in software versions 4.8.9 and below

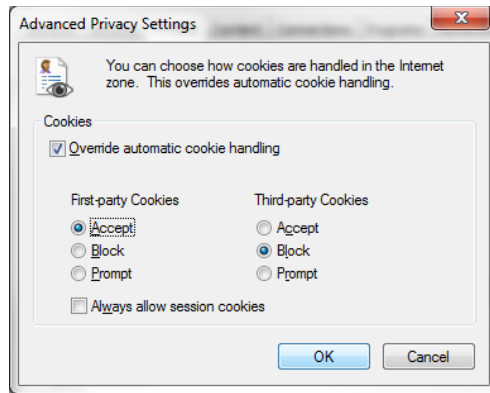
- Versions 4.8.9 and below have a memory leak occurring when the units have been up for an extended amount of time. There isn't enough free memory available to run Apache.
- With a Telnet or SSH session, perform/capture the results of a “**free -m**” command to verify the free memory is less than about 100MB (about the minimum for Apache to be able to run).

**Note (status update):** this issue was fixed with the version 5.0.0 (and above) updates.

#### M) “Certificate Error” reported. Verify “first-party Cookies” aren't blocked

- Refer to: <https://kb.iu.edu/d/ajfi>
  - If cookies are blocked/disabled, the login page will report “**certificate error**” near the IP address and will just keep clearing the login name (won't allow access to the browser).

1. Internet Explorer: Enable “First party Cookies” in Tools -> Internet Options, Privacy tab, Advanced button:



## 2. FireFox

- Enable “First party Cookies” in Tools -> Options, Privacy tab, History drop-down
- To allow sites to set cookies on your computer, select Accept cookies from sites. To specify which sites are always or never allowed to use cookies, click Exceptions.
- To view or remove individual cookies, click “remove individual cookies”

---

## N) Web browser very slow/sluggish or not available

### Possible reasons:

- LDAP and/or Radius, Tacacs (Remote Servers) Enabled, servers configured- but not accessible.
- If one or more LDAP or Radius servers are configured but not available (such as using a direct connect for instance), the login will be delayed while the time server tries to establish comms with each one. The timeout and number of retries for each server will primarily determine how long it will take to login locally. Local login doesn't occur until all configured Radius and/or LDAP servers have been contacted and timed-out.
- KTS stopped running- is the front panel time still incrementing?
- 1<sup>st</sup> gen ETX Module installed.
- Bad ETX module.
- Memory leak in versions 4.8.9 and below (if CLI is still available, type version <enter>) More on this further below.
- Lots of processes on the “outer processor” (ETX module) such as NTP, multiple SNMP connections, several simultaneous web browser connections, etc.

---

## O) “ERROR: The web server encountered an unexpected error and failed to display the page you requested.”

This error message may be displayed if the SecureSync isn't available yet. Also, deleting “cgi-bin/StatusConfig.cgi” after the SecureSyncs IP address/DNS name in the web browser address field (leaving just https:// and the address) may also help.

### Using Chrome

(Refer to case 6452) Mark Dion reported that in Chrome, each time he selects a main menu, it keeps taking him back to the login screen. I spoke to Paul Myers and he recommended he make sure that screen/page caching is not enabled. It should be configured for refresh on each new page/screen.

Regarding the condition you reported when accessing the SecureSync using Chrome, I wanted to let you know I had a moment to discuss this condition with one of our engineers.

He mentioned that he hasn't ever seen or heard of anyone else seeing this abnormal web browser operation. He said it sounds like your browser may be currently configured to cache pages/screens. It is recommended that whichever browser is used to access the SecureSync (IE, Firefox or Chrome), that the browser be configured with no page caching. It should instead be configured with "refresh with each new page" (I'm not sure where this setting is in Chrome).

Please let me know either way, if you had screen/page caching enabled in Chrome, and if turning it off resolved this issue. OR, if you have any other questions or if you need anything else from us (now or in the future), please don't hesitate to let me know!

---

## P) Web browser failing after login (due to memory leak in 4.8.9 and below)

- Use **df -h** cli command to verify CF card isn't too full

```
spadmin@Spectracom ~ # df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M   53% /
/dev/hda1       963M  480M  434M   53% /
devtmpfs        248M    0  248M    0% /dev
```

If you can connect/login to the CLI interface (via ssh or telnet, or via a serial cable connected to the DB9 port on the front of the unit), there are a couple of commands to issue.

After logging in, first perform a **defcert** <enter> command (as shown below). Then try logging in again via the browser (can keep the connection to the CLI open). This command resets the HTTPS certificate.

- Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
- Example syntax is **defcert -sha256**
- V5.6.0 also changed the default algorithm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).

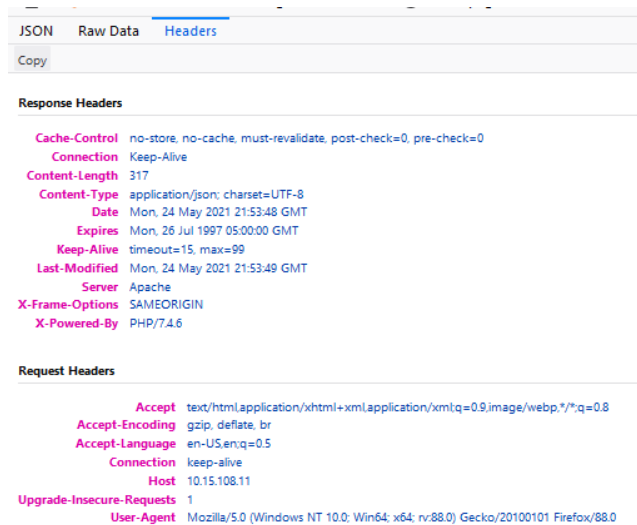
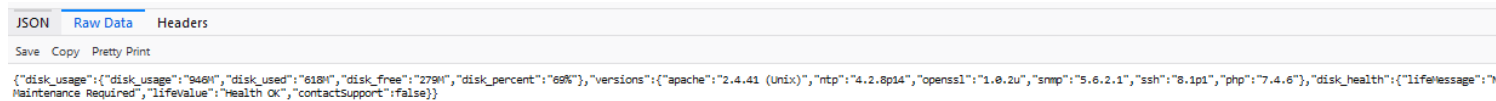
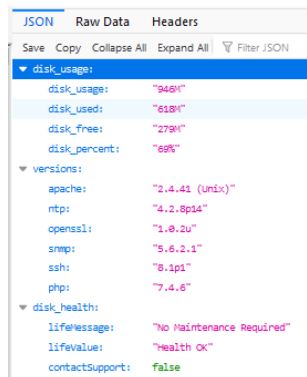
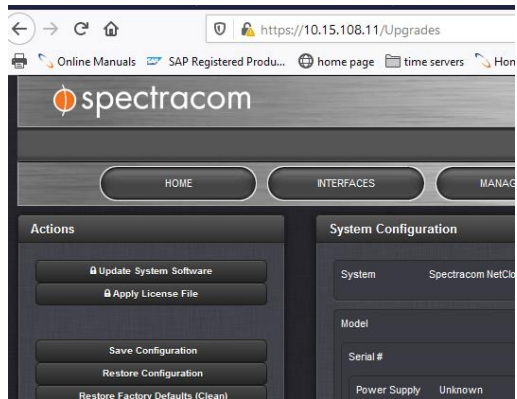
If defcert doesn't restore access to the browser, perform a **servset 6 off** <enter> command followed by **servset 6 on** <enter> (as shown below). Note the two servget commands in the screenshot are optional). This will restart just the web browser service alone.

```
8=NIP service
spadmin@CustService-176 ~ # servset 6 off
spadmin@CustService-176 ~ # servget 6
HTTPS Service      disabled
spadmin@CustService-176 ~ # servset 6 on
spadmin@CustService-176 ~ # servget 6
HTTPS Service      enabled
spadmin@CustService-176 ~ #
```

Please let me know if either of these commands restore access to the browser!!! Thanks!

## Specific examples where REST API can be used

Note: perform the desired function in the browser of a SecureSync, and add `.json` to the very end



## General info about retrieving status info from the browser

(email from Ron Dries 9 June 2021)

For the GNSS status what I would recommend is right clicking on the GNSS 0 item in the menu opening it in a new tab, and then appending `.json` to it.

That will show you the `.json` data for that.

Now this only works for pages that include all of the data on them from one call.

The **System Status** is handled differently and is an element on the page.

For request that you can't find easily by appending .json, I would recommend still sending the requests to the Apps team as we can help to chase down the correct Endpoint, or we have it already due to having someone else already request it.

Depending on the skill level of the customer, it is possible to find this information utilizing the developer tools that web browsers have accessible.

However this can take time which is why I still recommend sending it to the Apps team for assistance.

For your point about the **Home** page to see the JSON data it provides you need to use the Endpoint: /home.json.

When you login to the UI there is a specific Home page it is usually just hidden in the url and you are automatically routed to the Home page.

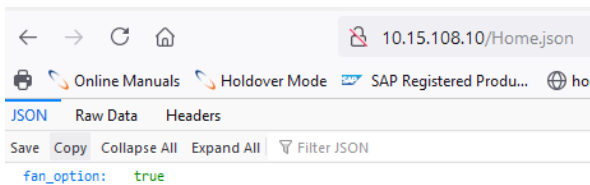
### Finding "Feature Numbers"(for various \*tabs"/pop-up menus on a browser page)

1. After opening a page, **Right-click** on the desired tab or Gear Icon, and "**Open Link in new tab**".
- 2.url at top of page will report the Feature Number


---

### Accessing info from the Home page of the browsre

- Normally, the url for the Home page just reports the IP address.
- From Ron's email futher above: "For your point about the **Home** page to see the JSON data it provides you need to use the Endpoint: **/Home.json**"

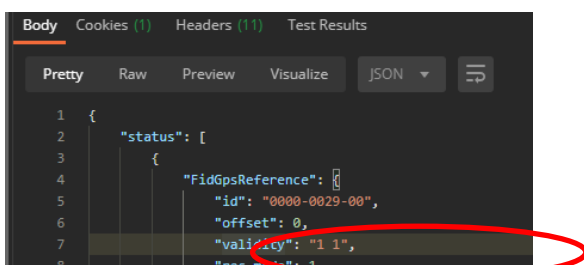


### "Performance" sub-section of the Home page

1. Right-click in the "two arrows" Icon 
2. Selefct "**Open Link in new tab**"

---

### "validity" variable



The variable “validity” is the Time and 1PPS validity.

So as an example:

“validity”: “1 1” – means Time is valid “1” and 1PPS is valid “1”

“validity”: “1 0” – means Time is valid “1” but 1PPS is invalid “0”

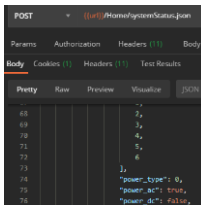
---

## Specific info for retrieving Status info

### Retrieve Status info

#### 1. Power (as reported in *Home-->System Status-->Power*)

**Email from Ron D (7 June 2021)** To get both Power and System Status from the Home page a GET request can be sent to the Endpoint: `/Home/systemStatus.json`



#### 2. Home-->System Status-->Status

**Email from Ron D (7 June 2021)** To get both Power and System Status from the Home page a GET request can be sent to the Endpoint: `/Home/systemStatus.json`

### A) Poll Time info

- To get time info, use the Endpoint: `/Features/getTime.json`

### B) Poll current GNSS position

- Position can be queried from the GNSS status Endpoint: `/Features/status/0000-0029-00.json`

### C) Poll 1PPS Phase Error data

- Refer to: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API - Postman and Python scripts\Python scripts\poll phase error data](#)

### D) IRIG and ASCII outputs

- Refer to: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API - Postman and Python scripts\Python scripts\IRIG and ASCII outputs](#)

### E) 10 MHZ and 1PPS outputs



➤ Refer to Salesforce case 25034

➤ Refer to:

Q We have a customer (BAE in Los Angeles) that wants to turn on and off the 10 MHz and 1PPS outputs using the CLI. It appear we have the command for 1PPS **ppsctrl**, but I didn't see one for 10 MHz – is there one

**A Email from Dave S (12 Apr 17)** These configurations can also be adjusted via the REST API that we are continuing to document. Any 1PPS or 10MHz in the system could be controlled in this way.

## F) Download GPS/GNSS 0 receiver status info (as reported in [Home-->Reference Status-->GNSS Status](#))

Refer also to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts\Python scripts>

### 1. Via REST API interface

➤ Refer to Salesforce cases such as 270348

➤ The REST API endpoint for GNSS Status info

**Email from Ron D (7 June 2021)** To get GNSS Status a GET request can be sent to the Endpoint: </Features/status/0000-0029-00.json>



```
POST {{url}}/Features/status/0000-0029-00.json


Parameters Authorization Headers (1) Body Pre-requests

Body Cookies (1) Headers (1) Test Results

Pretty Raw Preview Visualize JSON

1 {
2   "status": [
3     {
4       "fidGpsReference": {
5         "id": "0000-0029-00",
6         "offset": 0,
7         "validity": "1 1",
8         "rec_mode": 1,
9         "rec_dyn": 0,
10        "nSats": 13,
11        "sat_data": {
12          "svids": [
13            "G01",
14            "G07",
15            "G08",
16            "G13",
17            "G14",
18            "G15",
19            "G17",
20            "G21",
21            "G27",
22            "G28",
23            "G30",
24            "E01",
25            "E04",
26            "E09",
27            "E13",
28            "E14",
29            "E21",
30            "E26",
31            "E31"
32          ],
33          "data": [
34            21,
35            21,
36            -
```

Add ".json" to the endpoint in the browser, for a list of all GNSS parameters (such as shown below) available via Rest API.

 [10.15.108.10/Features/status/0000-0029-00.json](http://10.15.108.10/Features/status/0000-0029-00.json)

```

status
0
FidGpsReference
id "0000-0029-00"
offset 0
validity "0 0"
rec_mode 1
rec_dyn 0
nSats 0
sat_data
svids []
data []
colorMap []
survey_prog "99"
manufacturer "u-blox M8T"
constellation 9
antenna "2"
latitude "43.041230"
longitude "-77.675033"
altitude "175.823000"
gen_rinex_yuma false
mode_ldescription "Standard"
dyn_ldescription "Land (Resurvey)"
survey_ldescription "99%"
survey_complete false
antenna_ldescription "Open"
cnst_ldescription "GPS Galileo "
gps_cnst true
glo_cnst false
bei_cnst false
gal_cnst true
qzs_cnst false
num_receiver_channels 12
license_agps false
en_agps_client false
rinex_poll_period "10"
yuma_once_aday false
yuma_poll_time "12:00"
yuma_poll_period "10"
station_name "spec"
record_days "7"
en_agps_server false
agps_data_client false
agps_data_server false
schema
offset
id 0
name "offset"
title "Offset"
readable true
getParams ""
isStatus true
isSetting true
setBasic false
logBasic true
parentName false
type "nanoseconds"
null true
default null
length 0
validity
id 2
name "validity"
title "Validity"
readable true
getParams ""
isStatus true
isSetting false
setBasic false
logBasic true
parentName false
type "validity"
null true
default null
length 0
rec_mode_dyn
id 4

```

```

name          "rec_mode_dyn"
title         "Receiver Mode Dyn"
readable      true
getParams     ""
isStatus      true
isSetting     true
setBasic      false
logBasic      true
parentName    false
type          "subfield"
null          true
default       null
length        0
getResults    0
              "rec_mode"
              1
              "rec_dyn"
setParams     0
              "rec_mode"
              1
              "rec_dyn"
rec_mode
id            4
name          "rec_mode"
title         "Receiver Mode"
readable      true
getParams     ""
isStatus      true
isSetting     true
setBasic      false
logBasic      true
parentName    "rec_mode_dyn"
type          "enum"
null          true
default       null
length        0
range         "enumReceiverMode"
rec_dyn
id            4
name          "rec_dyn"
title         "Receiver Dynamics"
readable      true
getParams     ""
isStatus      true
isSetting     true
setBasic      false
logBasic      true
parentName    "rec_mode_dyn"
type          "enum"
null          true
default       null
length        0
range         "enumDynamics"
fix_data
id            6
name          "fix_data"
title         "Fix Data"
readable      true
getParams     ""
isStatus      true
isSetting     false
setBasic      false
logBasic      true
parentName    false
type          "subfield"
null          true
default       null
length        0
getResults    0
              "nSats"
              1
              "pdop"
              2
              "hdop"
              3
              "vdop"
              4
              "tdop"
              5
              "fom"
              6
              "tfom"
              7
              "herr"
              8
              "verr"
nSats

```

```

id          6
name       "nSats"
title      "Number of Tracked Satellites"
readable   true
getParams  ""
isStatus   true
isSetting  false
setBasic   false
logBasic   true
parentName "fix_data"
type       "integer"
null       true
default    null
length     0
sat_data
id          7
name       "sat_data"
title      "Satellite Data"
readable   true
getParams  ""
isStatus   true
isSetting  false
setBasic   false
logBasic   true
parentName false
type       ""
null       true
default    null
length     0
survey_prog
id          8
name       "survey_prog"
title      "Survey Progress"
readable   true
getParams  ""
isStatus   true
isSetting  false
setBasic   false
logBasic   true
parentName false
type       ""
null       true
default    null
length     0
manufacturer
id          11
name       "manufacturer"
title      "Manufacturer/Model"
readable   true
getParams  ""
isStatus   true
isSetting  true
setBasic   false
logBasic   true
parentName false
type       ""
null       true
default    null
length     0
constellation
id          21
name       "constellation"
title      "Receiver Constellation"
readable   true
getParams  ""
isStatus   true
isSetting  true
setBasic   false
logBasic   true
parentName false
type       "enum"
null       true
default    null
length     0
range      "enumReceiverCnst"
antenna
id          18

```

|            |                 |
|------------|-----------------|
| name       | "antenna"       |
| title      | "Antenna Sense" |
| readable   | true            |
| getParams  | ""              |
| isStatus   | true            |
| isSetting  | false           |
| setBasic   | false           |
| logBasic   | true            |
| parentName | false           |
| type       | ""              |
| null       | true            |
| default    | null            |
| length     | 0               |
| position   |                 |
| id         | 3               |
| name       | "position"      |
| title      | "Position"      |
| readable   | true            |
| getParams  | ""              |
| isStatus   | true            |
| isSetting  | true            |
| setBasic   | true            |
| logBasic   | true            |
| parentName | false           |
| type       | "subfield"      |
| null       | true            |
| default    | null            |
| length     | 0               |
| getResults |                 |
| 0          | "latitude"      |
| 1          | "longitude"     |
| 2          | "altitude"      |
| setParams  |                 |
| 0          | "latitude"      |
| 1          | "longitude"     |
| 2          | "altitude"      |
| latitude   |                 |
| id         | 3               |
| name       | "latitude"      |
| title      | "Latitude"      |
| readable   | true            |
| getParams  | ""              |
| isStatus   | true            |
| isSetting  | true            |
| setBasic   | true            |
| logBasic   | true            |
| parentName | "position"      |
| type       | "position"      |
| null       | true            |
| default    | null            |
| length     | 0               |
| longitude  |                 |
| id         | 3               |
| name       | "longitude"     |
| title      | "Longitude"     |
| readable   | true            |
| getParams  | ""              |
| isStatus   | true            |
| isSetting  | true            |
| setBasic   | true            |
| logBasic   | true            |
| parentName | "position"      |
| type       | "position"      |
| null       | true            |
| default    | null            |
| length     | 0               |
| altitude   |                 |
| id         | 3               |
| name       | "altitude"      |
| title      | "Altitude"      |
| readable   | true            |
| getParams  | ""              |
| isStatus   | true            |
| isSetting  | true            |
| setBasic   | true            |
| logBasic   | true            |
| parentName | "position"      |

|                |                             |
|----------------|-----------------------------|
| type           | "position"                  |
| null           | true                        |
| default        | null                        |
| length         | 0                           |
| gen_rinex_yuma |                             |
| id             | 25                          |
| name           | "gen_rinex_yuma"            |
| title          | "Generate Rinex/Yuma files" |
| readable       | true                        |
| getParams      | ""                          |
| isStatus       | true                        |
| isSetting      | true                        |
| setBasic       | false                       |
| logBasic       | true                        |
| parentName     | false                       |
| type           | "boolean"                   |
| null           | true                        |
| default        | null                        |
| length         | 0                           |
| feature        |                             |
| SysFeature     |                             |
| id             | 41                          |
| visible        | true                        |
| is_reference   | true                        |
| is_output      | false                       |
| model          | "FidGpsReference"           |
| Feature        |                             |
| bi             | 0                           |
| fid            | 41                          |
| version        | 0                           |
| slot_id        | 0                           |
| card_id        | 0                           |
| card_version   | 0                           |
| instance       | 0                           |
| sys_instance   | 0                           |
| kts_ref        | "gps0"                      |
| sys_ref        | "GNSS 0"                    |
| id             | "0000-0029-00"              |
| description    | "GNSS Reference 0"          |
| license        | false                       |

---

## G) GPS jamming/spoofing info via REST API (only available if Opt-BSH is installed)

### 1. IF Opt-BSH is installed, Apps team can provide an endpoint to get status info from the Opt-BSH UI (within the SecureSync's browser)

- Refer to Salesforce Case 270348

**Summary email from Ron Dries (30 July 2021) for 270348** They asked to get status of jammed or spoofed, If they have BroadShield they can get this from the alarms provided at the Endpoint /home/systemstatus.json.

Position can be queried from the GNSS status Endpoint: /Features/status/0000-0029-00.json

To get time they can use the Endpoint: /Features/getTime.json

If they have BroadShield we can provide them an Endpoint to get the status information from the BroadShield UI, if they don't have BroadShield currently the Endpoint won't be useful to them.

### 2. Via .CSV file

- "Here is a simple python script (without error checking) to login and extract the GPS information and put it in a csv file."
- Refer to scripts in: [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API - Postman and Python scripts\Python scripts\GNSS receiver](#)

## H) Modify the input reference priority table

### 1. Refer to Case 195963

Q I'm looking for more info on the above API call to edit the ref priority table.

Given the below table (obtained from the same API URL) how would I structure the body of the API POST to disable, for example, the entry with 'id': '0.4' ? Anything I do seems to just create a new reference in the table. Do I have to pass in the entire table containing the edit?

```
{'data': [{'ReferencePriority': {'bi': 0,
'enab': True,
'id': '0.0',
'pps': 'gps0',
'prio': 1,
'time': 'gps0'}},
{'ReferencePriority': {'bi': 0,
'enab': True,
'id': '0.1',
'pps': 'epp0',
'prio': 2,
'time': 'hst1'}},
{'ReferencePriority': {'bi': 0,
'enab': True,
'id': '0.2',
'pps': 'hst1',
'prio': 3,
'time': 'hst1'}},
{'ReferencePriority': {'bi': 0,
'enab': True,
'id': '0.4',
'pps': 'hst0',
'prio': 4,
'time': 'hst0'}},
{'ReferencePriority': {'bi': 0,
'enab': True,
'id': '0.5',
'pps': 'hst0',
'prio': 5,
'time': 'hst0'}}]}
```

**A From Ron Dries (May 24, 2019)** Yes the table needs to be passed in with the edit they would like to make.

For them to edit the reference priority table they need to use the /References/edit.json API endpoint.

The order in which the references are in the JSON array that they send to this endpoint is the priority they will be in.

By setting the enable flag to false that will disable that entry. So for them to disable id 0.4 they would need a JSON array that has all of the references in the order they would like them to be in and set the enab flag to false for id 0.4.

For example:

```
{ "0" : { "ReferencePriority" : { "id" : "0.0", "enab" : true } },
"1" : { "ReferencePriority" : { "id" : "0.1", "enab" : true } },
"2" : { "ReferencePriority" : { "id" : "0.2", "enab" : true } },
"3" : { "ReferencePriority" : { "id" : "0.3", "enab" : true } },
"4" : { "ReferencePriority" : { "id" : "0.4", "enab" : false } },
}
```

Sending this in the body to the /References/edit.json endpoint will keep the priorities the same and change the enable flag for the reference with id 0.4.

---

## I) Get a specific log, or all logs

- The following endpoint can be used to send a GET request to query the log messages from a specified file:  
[/Logs/load/{logfile}.json](#)
- Refer to Salesforce Case 264688

To add to my earlier response about the REST API interface with SecureSyncs, I need to provide you with the Endpoints for obtaining all the SecureSyncs log files...

The following endpoint can be used to send a GET request to query the log messages from a specified file: **/Logs/load/{{logfile}}.json**

Where {{logfile}} is the name of the log file you want to query the messages from (such as the Alarms log, for instance)

For example: to get the messages from the Alarms log, the GET query can be sent to **/Logs/load/alarms.json**

You can send a GET request to the following endpoint to see the names of all of the available log files in the UI: **/Logs/index.json**

In the returned JSON array below, the values for the “log” key are what the **{{logfile}}** variable needs to be.

---

## Apparent Issues associated with REST API

### 1. 500 web UI error

- Fixed in Version 5.7.0 [JIRA ticket SSS-262] – “500 web UI error with REST API”

---

## Python Scripts/Scripting using REST API

Customers often want to run scripts to retrieve data from SecureSync. This isn't possible with the web browser itself. However (per Ron D) the REST API allows anything available via the browser to be scripted, using programs such as python.

### Info on python

<https://www.jetbrains.com/help/pycharm/step-1-creating-and-running-your-first-python-project.html>  
available for Windows or Linux as a free install

Online tutorial: <https://docs.python.org/3.6/tutorial/appetite.html>

### running a Python Script:

1. Copy the script file to the PC (such as in **c:/temp** for instance)
2. Open Windows command prompt window (**start -> run** and type **cmd**)

“To run the script, issue at the Windows command prompt the following command on a PC that has python installed (<https://www.python.org/downloads/release/python-352/>).

```
py query_ntp_stats_csv.py -H <SecureSync IP address> -u <username> -p <password>  
py query_ntp_stats_csv.py -H 10.2.192.226 -u spadadmin -p admin123
```

## Python script login to a SecureSync

- Refer to Case 218941 and: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API - Postman and Python scripts\Python scripts\poll phase error data](#)
- Per Ron, “....There is a function in this script that shows how to login to the SecureSync”:

```
def login_post(browser):
```

```
    ...
```



## Attempts to login to the SecureSync UI, passing the username and password specified by the user.

'''

```
browser.post("https://" + args.hostname + "/Users/login.json", json={"User": {"username": args.username, "password": args.password}}, verify=False)
```

### Session Cookies/Cookie Jar

➤ We do not do anything with the cookies in our python example scripts

Q (from a customer) The project I am working on is finally getting around to developing a python app that needs to query multiple SecureSync units and display various items of interest on a GUI.

We have gone through the provided documentation below and are able to get it working in Postman without issue. When we move over to the python environment we start running into a problem which we believe comes down to the session cookie.

Please let me know if the following assumptions are correct:

- 1) Before you can query the units, you must send a login request with the username and password. This login request should respond back with a session cookie, which we see in Postman.
- 2) The session cookie will be used instead of the username and password for all requests going forward, and passed in the header of subsequent requests. We see this in Postman as well.

Using Postman to generate the python code for authentication we end up with the following code:

```
import requests

def ts_login():
    s = requests.Session()

    url = "http://time/users/login.json"
    payload = '{"User": {"username": "USER", "password": "PASS"}}'
    headers = {'Content-Type': 'application/json'}
    r = s.request("POST", url, headers = headers, data = payload)
    print(r.headers)
    print(r.cookies)
    print(r.text)
```

Running the code we get the following output:

From r.headers:

```
{'Date': 'Wed, 14 Oct 2020 14:17:08 GMT', 'Server': 'Apache', 'X-Frame-Options': 'SAMEORIGIN', 'Expires': 'Mon, 26 Jul 1997 05:00:00 GMT', 'Last-Modified': 'Wed, 14 Oct 2020 14:17:09 GMT', 'Cache-Control': 'no-store, no-cache, must-revalidate, post-check=0, pre-check=0', 'Content-Length': '16724', 'Keep-Alive': 'timeout=15, max=99', 'Connection': 'Keep-Alive', 'Content-Type': 'text/html; charset=UTF-8'}
```

From r.cookies:

```
<RequestsCookieJar[]>
```

From r.text:

```
<!DOCTYPE html>
<html>
<head>
<!-- Always force latest IE rendering engine or request Chrome Frame -->
<meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>
Spectracom </title>
```

There is a lot more HTML returned.

It appears that the session cookie is not getting returned as the RequestsCookieJar is empty or the cookie is getting returned in a way python requests.Sessions() doesn't capture.

Do you have any suggestions or guides on how to properly obtain the the cookie?

**A Reply from Dave L (14 Oct 2020) We do not do anything with the cookies in our python example scripts**

## \*\*\*\*web browser Idle login timeout (login time-out after no activity)

- Refer to online SecureSync user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/OPRTN/Utimeout.htm?Highlight=10%20minutes](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/Utimeout.htm?Highlight=10%20minutes)

### A) Newer (black/charcoal) web browser

#### 1. Versions 5.4.0 and above (newer browser)

- Update **version 5.4.0** added configurable time-out (and consistent timeout of the browser)
- Click “Web interface Settings” on the left side of the **Management** -> **Network** page
- Configured in “**Minutes**”
- Available timeout range is from **10 minutes** to **1440 minutes (24 hours)**
- A change to the time-out period doesn't take effect until the NEXT login (not while already logged-in)



#### 2. Versions 5.3.1 to 5.1.2 (newer browser)

- Internal use only: this value is configured in core.php (/srv/www2/app/Config)
- The timeout is supposed to be 60 minutes. But as of at least version 5.3.0 this timeout isn't working correctly.
  - Refer to Mantis case 3021 (28 Sept 2015- this case is now being worked on. I expect it to be fixed in 5.4.0, ~Jan 2016)
- (As of at least version 5.3.0) this timeout is currently NOT user configurable in the newer browser.
  - Keith added Mantis case 3020 requesting the hard-coded 60 minute idle timeout be changed to a user-configurable value, as it was with the classic interface browser
  - 28 Sept 2015 KW: this case is now being worked on. I expect this capability to be added in 5.4.0, ~Jan 2016

Q Is it possible to block a session, that is, determine how long it can be in the session? Regardless of timeout?

A Keith's response (27 Sept 2019) for at least 5.8.6 and below The available browser timeout (10 minutes by default) can't "block" a session, but it does determine how long a valid login session can be open for, before the user needs to login again \*(the session automatically ends and new session needs to be opened, when the timeout expires).

The SecureSync has the ability to block ALL HTTP and/or ALL HTTPS sessions, via the individual HTTP and HTTPS On/Off slider switches (when either slider switch is off, that service is completely disabled/port is closed) for more info on disabling all HTTP and/or HTTPS sessions, please refer to the SecureSync user guide at:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/ConfNWsettings.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/ConfNWsettings.htm)

Other than the requirement that a user must know/enter valid account credentials (username and password) the SecureSync does not have the ability to block only some/certain sessions. Other than account password being used to control access to the SecureSync, blocking sessions is handled by disabling the HTTP and/or HTTPS services, as mentioned above.

## B) Classic interface web browser

- User-configurable idle time-out via the **Tools** -> **User** page, **Security** tab, "Idle Timeout field"



- Factory default setting for the "Idle Timeout" field was "0" which prevented an idle timeout disconnect from ever occurring.
- Looks like one of the updates may have broken this timeout (it doesn't appear to be timing out in at least version 5.2.1). To alleviate this condition, disable the classic UI altogether in the **Management** -> **Network** page of the newer browser.

**Email Keith sent to a customer.** If you wish to alleviate the classic browser not timing out, you can disable the ability to access the classic interface altogether, via the newer web browser. To disable access to the classic interface browser, in the newer browser navigate to the Management -> Network page. In the bottom-left corner, change the slider switch for "Classic UI" to the OFF position. Port "8080" is now closed, so the classic interface browser is no longer accessible.

Q. In 5.1.4 is there an option to set an inactivity logout after so many minutes? I have searched through the manual and not found it.

**A. Reply from Dave Lorah (30 July 2014)** In firmware versions 5.0.0 to at least version 5.2.0, the new (black/charcoal) web browser **does not** have a control for the inactivity or "Idle Timeout". This is still available but only found when you switch to the "Classic" interface.

If you wish to alleviate the classic browser not timing out, you can disable the ability to access the classic interface altogether, via the newer web browser. To disable access to the classic interface browser, in the newer browser navigate to the **Management** -> **Network** page. In the bottom-left corner, change the slider switch for "Classic UI" to the OFF position. Port "8080" is now closed, so the classic interface browser is no longer accessible.

---

## Apache Web Server in SecureSync

- SecureSync (like NetClock 9300s/9200s) also uses the Apache web server.

### A) Obtaining Apache version info

#### 1. Obtaining Apache version based on SecureSync software version installed

- Refer to the “Software Release Date” spreadsheet at : [I:\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates](#)

#### 2. Obtaining Apache version via CLI command (telnet, ssh or RS-232)

- Version can be queried via the CLI (refer to Specific available CLI commands/API calls)
  - The command to get the Apache version is: **version web** <enter> (not “version apache”).

#### 3. Obtaining Apache version via the web browser

A) Software versions 5.1.7 and below:

- The Apache version isn’t displayed in the web browser.
- Obtain it via the CLI interface, instead.

### B) Software versions 5.2.0 (and above):

- Newer (black charcoal) browser: The Apache version is reported in the Tools -> Upgrade/Backup page
- **Classic interface browser:** The Apache version isn’t displayed in the classic interface browser. Obtain it via the CLI interface, instead.

---

## Web Server Vendor / Version Disclosure (Customer request to “hide” the Apache version, to prevent potential security vulnerability)

**Summary of the info below:** A customer requested the Apache version no longer be reported. Knowing the version installed could disclose potential vulnerabilities.

### Vulnerability Explanation

A typical web server response contains an HTTP Server header that reveals both the vendor and the version of the web server software. Additionally, third parties may inject headers disclosing supported software such as PHP or ASP. This information can lead an attacker to more focused attacks.

### Remediation - NTP not a windows box, will need to ask spectrum

Sequiris Group recommends that SRPMIC scrub the response headers before they are returned to the user. Microsoft has released a utility (URLScan) that helps modify headers before being sent to the requesting client. Please see the following URL for additional details: <http://www.iis.net/downloads/microsoft/urlscan>

Or

Can Spectracom edit the host file or related file on the Spectracom device to change or hide vendor information?

**Email from Paul Myers (6 Mar 17) regarding SecureSyncs/9400s (at least 5.5.1 and below)** In regards to hiding the Apache web server version information, we are reviewing this security recommendation internally with the Product Manager to see if we can fix this via Apache configuration in a future release.

---

## Apache Web browser page refresh

### “Classic Interface” Web browser page refresh

- Web Page refreshes every 30 seconds

### Refresh while in a sub-tab of each main web page

**Email from Dave Sohn on 5/9/11 (at least version 4.5.0 and below)** There is a known issue that a refresh on any page with tabs will return you to the first tab.

---

## Log entries for Unsuccessful/Successful browser logins

- Refer also to the “auth.log” section of this document: [Auth log \(Authentication log\)](#)

### Auth log (from PAM, not Apache) doesn't record successful browser logins (just successful SSH logins)

- Refer to <https://www.netbsd.org/docs/guide/en/chap-pam.html>  
<http://web.archive.org/web/20091229050456/http://www.sun.com/software/solaris/pam/pam.admin.pdf>

Q Can the Authorization log be set to record successful logins and logouts?

A The Auth (Authorization) log is a log generated and maintained exclusively by the PAM module (Pluggable Access Module) PAM is the software module we use for login (The Auth log is not a “Spectracom” log). The Auth log has entries asserted for failed web browser and CLI (telnet, ssh, etc) logins. It also has entries asserted for successful CLI Logins. However, the PAM module does not assert any log entries for successful web browser login.

If a successful login occurs and the user makes any changes while logged in, these changes (including the user account name, date and time is recorded in the Journal log (displayed in the **Tools -> Journal** page of the browser).

Note that the SecureSync also support remote authentication via Tacacs, LDAP and/or Radius. These remote Auth servers may have their own logging capabilities to record successful logins.

Note that the SecureSync also support remote authentication via Tacacs, LDAP and/or Radius. These remote Auth servers may have their own logging capabilities to record invalid logins.

## (Lafayette database) MySQL/SQLite databases and DB browser

### Directory to Lafayette database/checking file size of the database

Obtaining this file size can be performed via a CLI connection (ssh). After logging into the SecureSync:

1. CD to the following directory: `/srv/ww2/app/webroot`
2. Type the following command (as shown in the screenshot below): `du -s * | sort -nr | head`

```
spfactory@cdcntp201 /srv/ww2/app/webroot $ du -s * | sort -nr | head
233120 backup.sql
81284 lafayette_backup
81284 lafayette
1144 util
1016 img
896 images
712 js
300 css
292 font
268 favicon.ico
spfactory@cdcntp201 /srv/ww2/app/webroot $ rm backup.sql
spfactory@cdcntp201 /srv/ww2/app/webroot $ rm lafayette_backup
spfactory@cdcntp201 /srv/ww2/app/webroot $ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda1       947M  482M  416M   54% /
devtmpfs        10M    0   10M    0% /dev
tmpfs           50M  436K   49M    1% /run
shm             248M    0   248M    0% /dev/shm
cggroup_root    10M    0   10M    0% /sys/fs/cgroup
spfactory@cdcntp201 /srv/ww2/app/webroot $
```

### Removing the backup.sql file

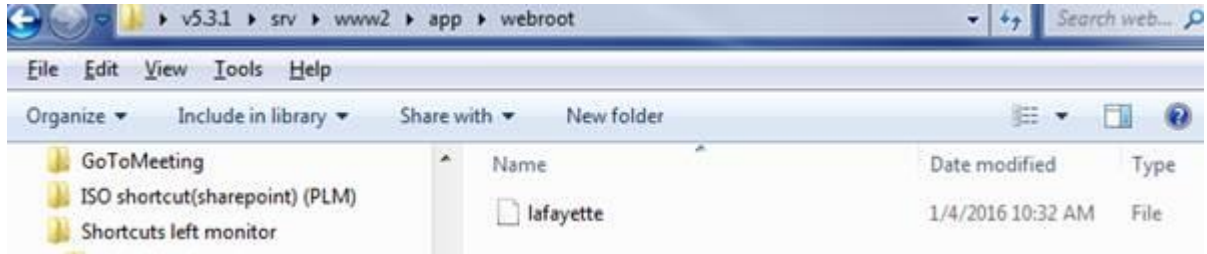
```
spfactory@cdcntp201 /srv/ww2/app/webroot $ du -s * | sort -nr | head
233120 backup.sql
81284 lafayette_backup
81284 lafayette
1144 util
1016 img
896 images
712 js
300 css
292 font
268 favicon.ico
spfactory@cdcntp201 /srv/ww2/app/webroot $ rm backup.sql
spfactory@cdcntp201 /srv/ww2/app/webroot $ rm lafayette_backup
spfactory@cdcntp201 /srv/ww2/app/webroot $ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda1       947M  482M  416M   54% /
devtmpfs        10M    0   10M    0% /dev
tmpfs           50M  436K   49M    1% /run
shm             248M    0   248M    0% /dev/shm
cggroup_root    10M    0   10M    0% /sys/fs/cgroup
spfactory@cdcntp201 /srv/ww2/app/webroot $
```

## Available SQLite database browser

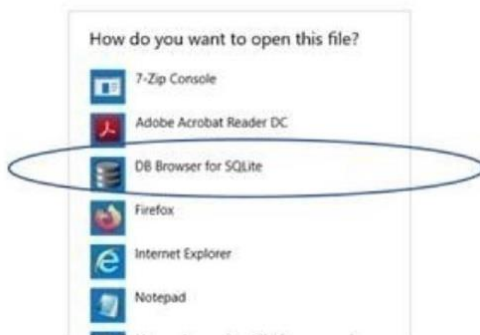
- Web browser available for SQLite (log bundles saved in versions 5.3.1 and above): “**dB browser for SQLite**” <http://sqlitebrowser.org>

- 1) **Sqlite Database (“Lafayette”)** is located in the “**SRV**” folder of the logs bundle (available after untarring the log bundle).

Note this file is a few folders into the srv folder (**srv/www2/app/webroot**). Just keep clicking each folder inside the srv folder, until you see this single file (as shown below):

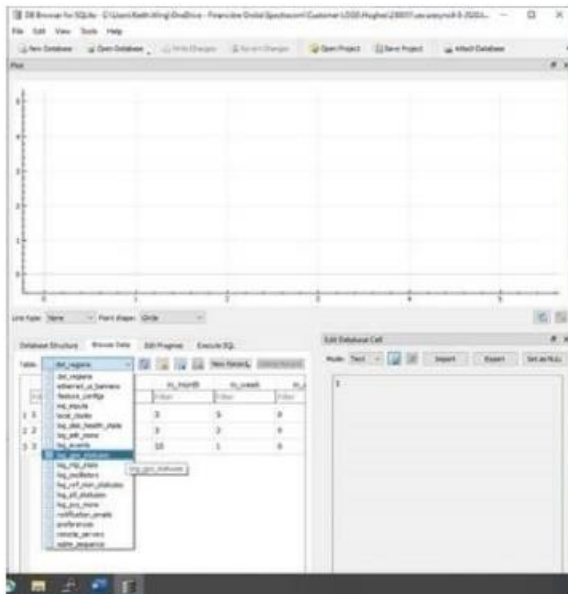


- 2) Double-click the “Lafayette” fi; and select to open it using the “DB Browser for SQLite” program.



- 3) Under the graph area, select the “Browse data” tab

- 4) Change the “table” to the desired type of data to graph:



For instance:

- **log\_gps\_statuses** table: provides GNSS satellites tracked and SNR strength values

- **log\_oscillators table:** provides DAC values, Phase Errors, etc.

- Select the “Browse Data” tab and then select “log\_oscillators” in the “Table” drop-down at the top of the tab.
- To plot oscillator data, select View-> Plot (at the top of the page). At the top-right, select the desired columns.

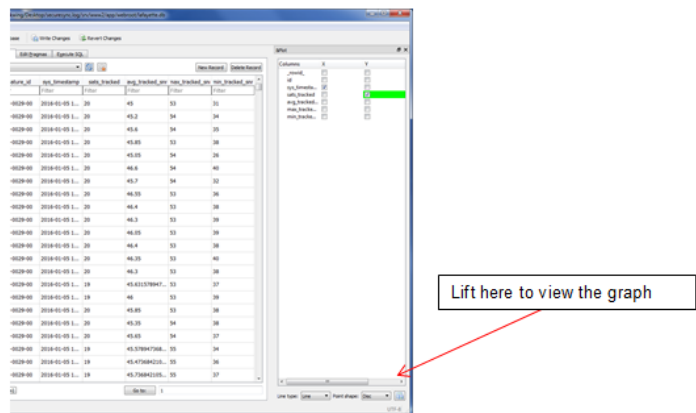
**Note:** Select either ID or RowId for the X and desired value(s) to graph in Y column. Graph updates automatically.

**To view/plot (graph) satellite data for instance:**

- Select the “Browse Data” tab and then select “log\_gps\_statuses” in the “Table” drop-down at the top of the tab.
- To plot satellite data, select **View-> Plot** (at the top of the page). At the top-right, select the desired columns.

**Note:** Select “**sys\_timestamp**” for the X column and desired value(s) to graph in Y column. Graph updates automatically.

**Note:** if the graph can't be found in the screen (and if **View -> Plot** has been selected) move the Plot table to the right side of the screen and use the mouse to pull up on the bottom bar.



**Specific available selections/tables of data**

**A) Log\_ntp\_stats (ntp\_client and ntp\_server throughput stats)**

**B) Log\_sys\_mons: System Monitor info**

- **Load01, load02 and load03** : associated with CPU load – not NTP/network loading (these are memory values reported in the linux top command- I believe they are (in order left to right- VIRT, RES and SHR)
- **CPU\_used:** % CPU usage
- **Sys\_temp:**
- **Cpu\_temp:**

**C) Log\_oscillators (“discstats”: Sync, Holdover, selected Time/PPS references, DAC, Phase/freq errors, System/CPU temps)**

**Note:** Effects on Phase Error graphs if a GPS Offset has been configured in the browser

- Unlike the Phase Error data reported in “**log\_ref\_mon\_statuses**”, the Phase Error data in



“log\_oscillators” is based on raw (no offset applied) GPS.

- If any “GPS Offset” has been applied to the GPS configuration in the browser, Phase Error data reported in “Ref Monitor” will be offset by the value in the GPS Offset configuration (such as 800ns for instance). The Phase Error data in **Log\_oscillators** is based on raw (no offset applied) GPS.

**Example below (both graphs from same SecureSync) per Salesforce Case 255365**

**Email from Ron Dries (12 Jan 2021)** I looked at the logs and the sqlite data.

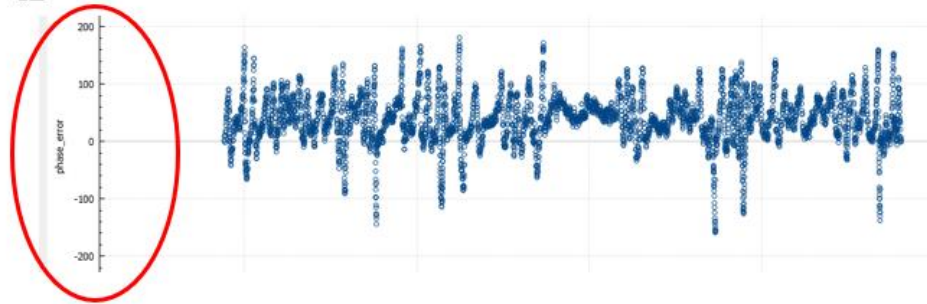
The difference between the phase error in log\_oscillators and the phase measured in the log\_ref\_mon\_statuses is due to having an offset configured for the GPS reference.

In journal.log.1 there are entries where they set the GPS offset from 600 to 897:

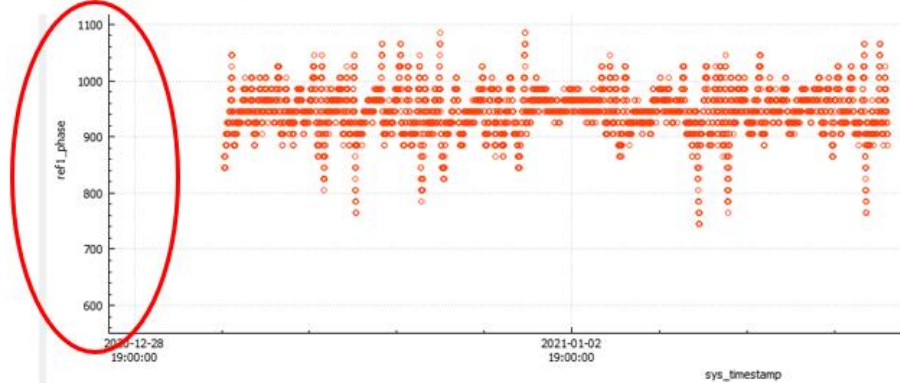
Feb 9 03:15:13 [webui] Changed Offset for GPS Reference 0 in slot 0 from GR (0)Offset: 600 to **GR (0) Offset: 897**

The reference monitor is a measurement taken before that offset gets applied

**A) log\_oscillators Phase Errors**



**B) log\_oscillators Phase Errors**



---

## General info regarding MySQL/Sqlite databases

- MySQL database was replaced by SQLite database in **version 5.3.1** update.
- ~~Qleg~~ (was) the primary point of contact for MySQL questions/issues
- MySQL database is located in the **/usr/bin** directory
- MySQL is an open source database that was added in version 5.1.0 to support the new, black/charcoal background browser.
- MySQL is a configuration database for the newer web browser (not the classic interface) that stores configurations (standard functionality for MySQL) and also logs data for generating our graphs in the newer browser (this is custom function we created for MySQL to store the graph data).
- Earlier versions of software (prior to version 5.1.4) had difficulty with the database repairing itself – it required a system reboot to repair.
- **Version 5.1.4** made the database more robust and allows it to repair itself without having to reboot.
- A problem with MySQL database typically only affects the web browser graphs.
- Since the database wasn't in software versions prior to version 5.1.0, the memory consumption issue in versions 4.8.9 and below is not a cause of MySQL error messages.
- Configuration storage in MySQL uses one connection to MySQL and the logging of data for the graphing functions in the newer browser uses a separate connection to MySQL.
- We periodically poll the GPS receiver for SNR and Number of tracked sats and poll the oscillator to log its data. This polling is completely separate to the standard SecureSync logs that are asserted (no correlation between the polling period and log entries being asserted).
- If something adverse was to happen to the MySQL connection while updating a configuration, MySQL has its own way of recovering from this without losing any info (recovery is built-into MySQL because this is a standard function of MySQL).
- If something adverse was to happen to the logging connection to MySQL while updating the logging data, MySQL doesn't have a way of recovering from this without potentially losing that one data point
- The logging connection can be lost at any point due to MySQL restarting to fix any of its errors.
- Starting in update version 5.14, we now verify the connection to MySQL for logging is good before we try logging any new data and will reconnect if not already connected. In versions prior to 5.1.4, the graphs in the browser just ended until the SecureSync was rebooted (The reboot re-established the connection).
- The log entry of **General error: 2006 MySQL server has gone away (WEB)** indicates the **logging** connection to MySQL was initially present but was lost while storing data. It doesn't try again to store the data.
- Whether or not that data at that poll is lost depends on when the connection to MySQL is lost.
- If the connection was lost at the beginning of the logging, the one data point was likely lost.
- If the connection was lost at the end of the logging, the one data point was likely stored.

Because the data is often polled and the data being graphed doesn't change much during the poll interval, it's highly unlikely that loss of data will be noticeable in versions 5.1.4 and above (graph data will just stop until reboot in versions prior to 5.1.4).

**Known issue:** Database file can continue to grow- causing issues with updating the software/extracting log bundle

- Refer to SecureSync release notes

---

**backup.sql file residing somewhere within the file system**

- This is a large (~150MB) unnecessary file which just a couple of customers have found in the file system (one was in Jul, 2017 and Morgan mentioned he has seen it once and they just deleted it during a remote connection for an untreated issue. See SF case 25682 for this earlier instance).
- This file was likely “left behind” during an earlier process (perhaps during a software upgrade??)
- The location of this file may change (so the cleaner file can’t remove it)
- If the file is in the /tmp directory, rebooting/power cycling the unit should delete the file.
- Otherwise, this undesirable/unnecessary file can be safely removed with the customer proving us with remote connection to the unit for us to delete the file, or by performing a ‘clean’ and then reconfiguring the unit (use caution restoring a backup config bundle. Depending on when the bundle was exported from the unit, this same file may be put back into the unit again).

**Email from Ron D (25 Jul 17)** I took a look at the cleaner tool and it doesn't look like it will remove this file. Currently the two ways to get rid of it would be remote access and delete it, or using the clean operation

**Email Keith sent to customer (25 Jul 17)** I just spoke with the engineer I had forwarded this info along to...

The backup.sql file isn't an “intentional” file that needed to be placed (and remain) in this directory. It was likely “left behind” at some point in the past during a process being performed at that time.

This file can be removed using a couple of different methods. The easiest and fastest is if you can make the SecureSync remotely accessible, by either putting it on the Internet and providing us with the login credentials, or by providing us with remote control of a PC on the same network as the time server. One of our Engineers can then use the PC to remotely remove this large file for you!

If remote access/control of a PC is not possible/not allowed, the other method is to perform a ‘clean’ command via the SecureSync's browser, its cli interface (ssh or telnet connection), or via its front panel keypad buttons (the clean command is listed in the cmd menu, which lets you cycle through the list via the up or down keypad buttons and the green checkmark key accepts the command). This will reset the time server back to its factory default configuration. This method is a bit more “intrusive”, as it will require the desired configurations to be restored (it would be like receiving a new unit from the factory and having to configure it as desired).

If you happen to have an earlier backup of the config files (from before this backup.sql file was created/left behind) the configs can alternately be automatically restored, once the network settings have been manually configured (thereby allowing network access to the browser to perform the restoring of the configurations).

Note a new CF card, which is pre-burned with the same version of software currently installed, could also be sent to you. But this would require the top cover be removed and the CF card swapped out. This is very similar to performing a clean command, which doesn't require any disassembly of the unit to gain access to the CF card. The unit could then be updated to version 5.7.0 (as the timing system software is not stored on the CF card, we can't send the CF card with 5.7.0 pre-burned. The main software on the CF card and the timing system software sub-assy need to be upgraded together, at the same time, to ensure they can continue communicating with each other).

Please let us know if you can provide either our Engineering team in France, or our team in the US, remote access to the SecureSync and we can then delete this file for you. Or, if you prefer to perform a ‘clean’ via the browser/cli or front panel and then just restore the configs, before updating the software to version 5.7.0. Then we can go from there!!!

I apologize for any inconvenience this condition may have caused!

---

## Oracle database (not used/applicable to SecureSyncs/9400s)

Q Basically we are concerned if our spectracom is actually using any Oracle as internal database? If we are not, then I can say the issue in the link provided are pretty much not applicable to us. I would just need a confirmation from the support side regarding this.

**A (Reply from Keith, 14 Nov 16, applies to at least version 5.5.0 And likely all versions beyond)** I can confirm for you that the SecureSyncs (as well as the 9400 series NetClocks) do not/have not, contained an Oracle database. Instead, it uses an SQLite database (earlier versions of software used a mysql database.- neither of these are from Oracle).

---

## Apache Struts and Apache Tomcat server

- As of at least version 5.7.1 (~Oct 2017) neither of these add-on programs (Apache Struts or Apache Tomcat server) are used in SecureSyncs/9400s, as confirmed by Engineering, and are not likely to start being used anytime in the future
- Any potential vulnerabilities directly associated with these available add-on programs do not apply

### A) Apache Struts

- Refer to <https://struts.apache.org/>
- Refer also to CVEs associated with Struts (such as “**CVE-2017-5638**”) in the Customerserviceassist doc.

Apache Struts is a free, open-source, MVC framework for creating elegant, modern Java web applications. It favors convention over configuration, is extensible using a plugin architecture, and ships with plugins to support REST, AJAX and JSON.

#### Email from Paul Myers (16 Mar 17)

<https://struts.apache.org/>

We don't include apache struts.

I don't see apache struts as part of Gentoo anyway.

We use apache web server.

**Email Dave sent to a customer (20 Aug 2020)** We don't include apache struts in our firmware in any Spectracom product.

We use the apache web server but it does not include the Apache Struts software. This CVE Apache Struts2 Vulnerability does not affect Spectracom Devices.

---

### B) Apache Tomcat server

**Email from Ron Dries (16 Oct 17)** Correct, SecureSync does not use Apache Tomcat.

---

## \*\*Web browser can't open (can't login at the login prompt or prompt not displayed) yet telnet and/or SSH is working

- Refer to the known issues for a list of reasons a user may not be able to login at the browser login prompt or may not get the prompt to login
- Good document for troubleshooting web browser/ssh issues:  
<https://www.linode.com/docs/troubleshooting/troubleshooting/>
- Review the Apache Error and Access logs

### Apache logs (Access and Error logs)

- For general info, refer to <http://httpd.apache.org/docs/2.2/logs.html>
- **error\_log** (Apache error log) and **ssl\_request.log** (Apache Access log)
- Starting in version 5.2.1, these logs are contained in the saved log bundle.
- Can also be viewed in the CLI in the **home/spectracom/log** directory.
- Refer to the “logs” section of this document for details on log entries.

## A) Apache Access log (ssl\_request.log)

“Apache uses the access log files to record information about every visitor to your site. You can see which files visitors view, how the web server responds to requests, and other information such as the web browsers visitors use.”

## B) Apache Error logs (error\_log)

“The error log is where Apache records information about any errors or anomalies it encounters. Many of the “errors” Apache records are typically minor, such as a visitor requesting a file that doesn't exist. Apache also uses the error logs to record warnings that can indicate a potential problem with a particular event or configuration.

First, change to the **home/spectracom/log** directory (type **cd log**)

Type **cat ssl\_request\_log.1** and then type **cat error\_log.1**

Copy/paste the responses to these two logs, and please send to me.

---

## Symptoms relating to possible issue with Apache

1. Can connect via telnet/ssh (rules out any likely network issues).
2. May be able to get to the login screen, but error occurs when trying to login.
3. May not be able to get to the login screen at all (Apache IS needed to be able to see the login screen).

---

## Summary to potentially fix issues with the Apache browser

1. Starting in version 5.2.1- Refer to the logs: error\_log and ssl\_request.log (both are associated with Apache) via either a saved log bundle or via the CLI in the **home/spectracom/log** directory
2. Any error messages displayed (more info on error messages further below).
3. Decrease the security settings of the customer's browser

**\*Note:** If the browser settings are set too high, no logs or indicators are generated in the time server. It just stays at the login page with no changes.

For example, Internet Explorer set to “High” security will block the browser connection, even though the SecureSync's logs indicate a successful connection (we can't sense the browser settings are too high, so we can't assert any error messages if this happens)

**Internet Explorer:** Tools -> Internet Options, Security tab -> Security level for this zone.

Note that:

- **Medium-high** should allow access.
- **High** will block access to the site.
  - 1) Reboot or power cycle.
  - 2) Perform a **servget 6** <enter>. Make sure it responds “**HTTPS Service Enabled**”.
  - 3) Perform an **rc-status** CLI command. See if two instances of “**Apache2**” are listed and “started”

```

spectracom spectracom # rc-status
unlevel: default
gbe-load [ started
net.eth0 [ started
net.eth1 [ inactive
net.eth3 [ inactive
mysql_db [ started
mysql [ started
kts [ started
identify [ started
sysklogd [ started
netmount [ started
apache2-cert ← [ started →
apache2 ← [ started →
logd [ started

```

- 4) Perform a **ps -el | grep apache** CLI command. Make sure Apache2 is listed

```

Spectracom spectracom # ps -el | grep apache
5 S 0 2101 1 0 80 0 - 13718 poll_s ? 00:07:32 apache2
5 S 1001 2116 2101 0 80 0 - 9415 skb_re ? 00:00:00 apache2
5 S 1001 2445 2101 0 80 0 - 15457 semtim ? 00:00:04 apache2
5 S 1001 2486 2101 0 80 0 - 14481 epoll_ ? 00:00:02 apache2
Spectracom spectracom #

```

- 5) Perform an **unrestrict** CLI command
- 6) Perform a **defcert** CLI command
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - Example syntax is **-sha256**
  - V5.6.0 also changed the default algorithm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).
- 7) Perform a **servset 6 off** and then a **servset 6 on**
- 8) Perform a **Force/Clean upgrade** using the **sysupgrade** CLI command

From the SecureSync Software update instructions (example below- file name may need to be changed):

- 1) Perform cli command: **sysupgrade force updatexxx.tar.gz** (where x is the version)
- 2) Perform cli command: **sysupgrade clean updatexxx.tar.gz** (where x is the version)
- 3) Get the logs using CLI (either FTP or cat the logs and copy/paste them)
- 4) Use the **savelog** CLI command to generate a bundle with all the logs (**savelog** followed by a file name, such as **SecureSync**)
- 5) FTP out this file from the **home/spectracom/xfer/log** directory and send to us.
- 6) Are there any KTS issues indicated in the logs (such as KTS time-out issues for example). KTS could be loading down the system, preventing the browser from being able to open.
- 7) **cd /var/log/apache2 cat error\_log.** (Note: Versions 4.8.9 and below only. With Versions 5.0.0 and higher, spadmin doesn't have permissions to apache2 folder. Refer to Mantis case 2906 ).
- 8) **Note:** Update version 5.2.1 added this log to the saved log bundle (refer to "error\_log" and "ssl\_request.log")
- 9) **/home/spectracom/log folder:** auth.log, daemon.log, kern.log, user.log.

The logs we would like to initially review are the following:

In the home/spectracom/log directory:

- auth.log
- kern.log
- user.log
- daemon.log



[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Users/logout), referer: http://10.2.100.176/  
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Users/logout), referer: http://10.2.100.176/  
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /toolsb) /contact), referer: http://10.2.100.176/  
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /tools/contact), referer: http://10.2.100.176/

## B) Normal entries for login to spadmin account

[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Home), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /users/login), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /users/login), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /users/login), referer: http://10.2.100.176/users/login  
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /users/login), referer: http://10.2.100.176/users/login

## C) Logs from a SecureSync exhibiting error 500 messages when logging in

enable, referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Not processing line, referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value then, referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value then, referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Premature end of script headers: StatusConfig.cgi, referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authmethod is currently (null) (for /spec500err.html), referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authtype is currently Pamacea (for /spec500err.html), referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=

## D) “RSA server certificate CommonName (CN) `Spectracom' does NOT match server name!?”

- Indicates web browser Security Settings may be set too high. Try lowering the settings to the lowest value and then login again.
- May need to replace the default HTTPS certificate with a new one using values particular to the network.

---

## \*\*\*\*No Error messages displayed when trying to login (stays at login screen)

- Try decreasing the security settings of the customer’s browser (such as Internet Explorer, Firefox or Chrome). Or try a different browser altogether

**\*Note:** If the browser settings are set too high, no logs or indicators are generated in the time server. It just stays at the login page with no changes.

For example, Internet Explorer set to “High” security will block the browser connection, even though the SecureSync’s logs indicate a successful connection (we can’t sense the browser settings are too high, so we can’t assert any error messages if this happens).



**Internet Explorer: Tools -> Internet Options, Security tab -> Security level for this zone.**

Note that:

- **Medium-high** should allow access.
- **High** will block access to the site.

#### \*\*\*\*Error messages displayed when trying to login/navigate between browser pages

##### A) "(Hostname) didn't send any data. ERR\_EMPTY\_RESPONSE"

- Refer to SF case 120558

**Reply from Dave L (26 Oct 17)** The Securesync may be suffering from a stalled web browser service. This can usually be restored by power cycling the unit. After power cycle the web UI should work again. Then perform a firmware update.

Here are some useful notes to help you with the update:

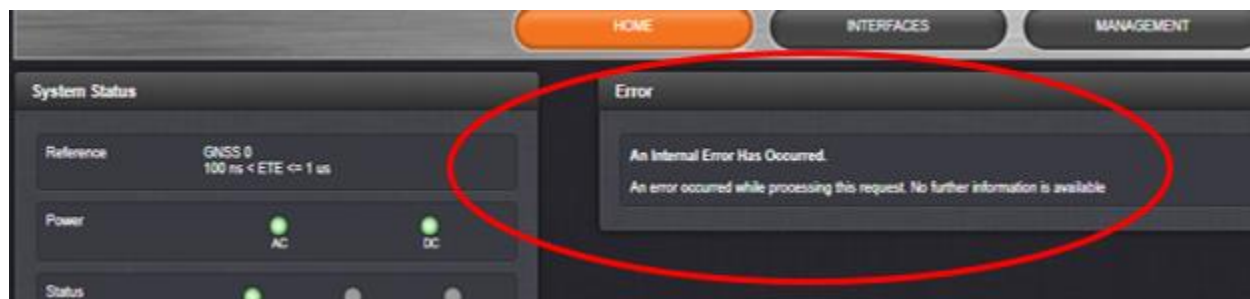
Make sure there are no older update files listed along with the new version 5.7.1 when you select it to perform the upgrade. If there are any others, select them and Delete Update file.

Run the updateCleaner file prior to performing the update. This will help clean out any old files that are taking up a lot of memory. Here is a link to get the updateCleaner: <https://files.spectracom.com/public-downloads/updatecleaner-securesyncnetclock-9400>

If the upgrade fails again, from the command line interface run the df -h command and make sure the memory used is less than 70%. It should be. IF not contact us and we can have a look as to why. This should result in a successful update. Please let me know how it goes.

##### B) Generic error 500 messages (can be reported as any of the below)

- "This error (HTTP 500 Internal Server Error) means that the website you are visiting had a server problem which prevented the webpage from displaying."
- "500 Internal Server Error"
- "HTTP 500 – Internal Server Error"
- "**Internal Server Error**"
- "**HTTP 500 Internal Error**"
- "**500 Error**"
- "**HTTP Error 500**"
- "An internal error has occurred. An error occurred while processing this request. No further information is available"
- **Note:** on at least one occurrence (18 Dec 2018, with v5.5.1 installed), this error message (**An internal error has occurred...**) was displayed ONLY when trying to navigate to **JUST** the **Management -> Time Management** page of the browser. All other pages were navigating just fine, with no errors displayed (recommended they reboot it-see the "software crash" email below).



#### Potential Solutions

##### A) Software crash/ with earlier versions such as v5.5.1

**Email from Dave L (8 Jan 18)** The Internal Server Error may be caused by a crash of the web service in the 9483. This can happen on rare occasions in older firmware versions such as 5.5.1. Typically a power cycle will restart the web service and restore communications.

Updating the firmware will help prevent this from happening in the future. We recommend updating to the latest version 5.7.1 which is available for free from our website. Here is a link to download the update and instructions.

<https://files.spectracom.com/public-downloads/latest-securesync-netclock-files>

IF the power cycle does not restore the web browser please let me know and we can explore a solution or RMA this 9483.

## B) Web browser time-out

**Email from Dave L (19 Sep 17)** It appears to me the web browser had timed out, causing the 500 Internal Server Error. Closing the web browser and reopening will resolve that issue.

- (v4.8.9 and below only) Use the CLI to type **version** <enter> and **free -m** <enter>. Then power cycle. If connection restored, or free is less than 100MB, likely caused by memory leak and should have software update applied.

(v5.x.x only) Use the CLI to perform a **df -h** <enter> to see if the CF card is full or nearly full.

- Use the CLI to obtain logs (such as the Auth log)
- Refer to sites such as the following:

**From:**

<http://kb.mediatemples.net/questions/1903/Why+am+I+getting+a+500+Internal+Server+Error+message%3F>

500 Internal Server Error is a generic error message, given when no more specific message is suitable. There are a number of causes for a 500 Internal Server Error to display in a web browser. Figure 1 is a sample error message.

**Email Keith sent to Salesforce case 15738:** To begin, “Error 500” messages are very generic messages that can be reported by the SecureSync’s web browser, if the browser can’t open. These messages are rare, but are typically related to a network issue of some sort and not likely an issue with the SecureSync itself. In this case, the SecureSync does not need to be rebooted to restore connection to the browser.

First, if you haven’t already attempted this, try connecting to the SecureSync via its CLI interface (such as by using telnet, ssh or FTP). As long as each service is enabled in the SecureSync (SSH is usually one that remains enabled), you should be able to successfully connect and login to the time server. If this connection also fails, it’s not just an issue associated with the browser. Also try just pinging the IP address of the time server, from the same PC trying to open its browser. If ping fails and the time server is on a different subnet, try pinging it from another PC on the same subnet as the time server. Does it respond to ping from both nodes?

If it doesn’t respond to ping from any PCs on the network, connect a PC directly to the SecureSync and try accessing it from this PC. If the Model 1204-06 Gb Ethernet Option Card is installed, and when connecting to Eth1, Eth2 or Eth3 on this option card, a network cross-over or straight network cable can be used (connecting to base Ethernet port Eth0 requires the use of a network cross-over cable). Temporarily configure the computer to have a static IP address on the same subnet as the time server’s address. Now try accessing the browser again. If the browser opens with this direct connection, there is a network related issue with the NetClock connected to the network that is preventing connection to the time server.

If it still doesn’t ping, try pinging a different Ethernet interface on the back panel, if the Model 1204-06 Option Card is installed. If it still doesn’t ping from another port, I recommend rebooting the server and see if then responds to pings and allows browser login. If it does, let me know and I will have you send us the logs to review, so that we can see if they indicate what might have caused this condition to occur.

Let me know what you find and then we can go from there.

## C) “[Fiddler] The socket connection to 10.2.100.176 failed. ErrorCode: 10060.

D) A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 10.2.100.176:80” (note the values in green will be the assigned IP address)

E) Time server is not accessible on the network. May have a network cable issue or it was recently rebooted.

Try connecting again in a couple of minutes. If still can't connect, might be a network issue or network is connected to a port of a Model 1204-06 Gb Eth card (Eth1,Eth2 Eth3) that is not enabled (issue the portstate get x <enter> CLI command to verify the current port state.

F) “ERROR: The web server encountered an unexpected error and failed to display the page you requested”

1. System memory leak occurring (versions 4.8.9 and below).

- Refer to: “Known issue: Apache Web browser no longer accessible, but can still ping, telnet etc still work.
- Power cycle or reboot to temporarily recover use of browser.

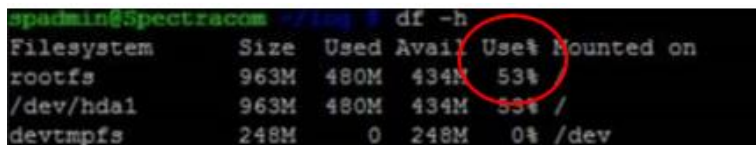
2. Potential SNMP issue (fixed in 4.8.0)

- Refer to: Known issue with SNMP in versions 4.7.0 and below
- Perform a clean command from Setup port to restore connectivity. Refer to Mantis case 1477 and Todd Belcher in PSalesforce. Note: An automatic reboot occurs when performing a clean command.

**Note:** This issue was fixed in software version 4.8.0.

G) An error occurred: Failed to insert session

- Check the CF card's disk usage (**df -h** in the CLI) to see if card is nearly full (especially with version 5.0.2 installed). May be full of nullmailers



```
spadmin@spectracom ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M  53% /
/dev/hdal       963M  480M  434M  53% /
devtmpfs        248M   0    248M   0% /dev
```

**Draft reply from Morgan:** Thank you for the information, we have a few other questions:

- 1) Can you access the device via the cli in interface (telnet or ssh session)?
- 2) What is the version of software currently installed ? (the CLI command is **version**) From your screenshot, it looks like it is version 5.0.2 or below.
- 3) Have you power cycled the time server?
- 4) If you can login via the cli, can you type the command (**df -h**) and let us know the percent used?

H) “An error occurred: @PAMSERVICE@ is not an authorized PAM service” displayed after entering username and password.

- Can be caused by memory leak issue in versions 4.8.9 and below (fixed in 5.0.0). Perform either a free or free mem command to see if the free mem is less than about 100MB (the min for Apache to run).
- Refer to Mantis case number 1339 <http://cvsmantis.int.rolia.com/mantis/view.php?id=1339>
- Can occur if there are issues with the HTTPS certificate in the Windows computer (try logging in with telnet/ssh. If this login is successful, the issue is likely with the HTTPS certificate).
- Can occur if username is entered in all caps (SPADMIN).
- Can occur if there are general issues with the network, preventing connection to the time server.

**Email Keith sent to Centurylink (1/28/13)** Did you happen to enter the user name in upper-case letters (SPADMIN) instead of lower-case letters (spadmin)? Entering the username in upper-case letters can cause this message to be displayed. The only other known reason to see this message is if there is a network issue that is preventing the PC from being able to access the NTP server.

If you enter the username in lower-case and still see this message, try telnetting into the unit (telnet xxx.xxx.xxx.xxx <enter> where x is the IP address of the NTP server). It should prompt you for a login, if telnet hasn't been turned off by a user, yet. (if it has been disabled, it should indicate the connection was refused).

### I) "Permission denied"

- Make sure the username is lower-case (spadmin) and not upper-case (SPADMIN).
- Wrong username and/or password may be being entered.

### J) glibc detected \*\*\* double free or corruption (!prev): 0x08053648

```
Spectracom login: spadmin
*** glibc detected *** double free or corruption (!prev): 0x08053648 ***
Spectracom login:
```

- "glibc detected \*\*\* double free or corruption (!prev): 0x08053648" displayed at login prompt (shown above)
- Reported by Robert Farrell w/Verizon (26 Feb 2014)
- Archive version 4.8.9 with 1204-06 card installed
- Appears to be the memory leak issue that was addressed in the version 5.0.0 update.
- Fix: update to versions above 4.8.9.

#### Paul Myers responded

This may be indicative of a memory problem possibly a memory leak or memory problem.

Is the Front panel updating?

Can they change the front panel screen operation?

Can the user login to the Web UI?

Can they login to the serial console?

Can they login SSH?

Can they FTP connect? (Probably not)

If the web ui is down too, they probably need to reboot, and update their unit to 5.1.2! It's very strange that you wouldn't be able to login, especially locally to the spadmin account, after applying the version 5.0.2 to 5.1.4 software update. I have a couple questions for you to better help you with this?

- 1) If the SecureSync has the Model 1204-06 Gb Ethernet Option Card (adds three additional Ethernet ports) installed, which Ethernet port are you trying to open the browser from (Eth0, Eth1, etc)? Note that after applying the version 5.1.4 update, Eth1, Eth2 and Eth3 are disabled in software. They can be disabled via the browser, if they are intended to be used, by logging into Eth0 (the base Ethernet port).
- 2) Are you able to ping the IP address of the SecureSync?
- 3) Are you able to access it over Ethernet via telnet/SSH?
- 4) When you try logging into the browser, do you get a login prompt?
- 5) If you get a login prompt, does it report any error messages when you try to login? What is displayed when you try to login?
- 6) If you get a login prompt, have you tried logging into the **spadmin** account using the factory default password of **admin123**?

**If you can access it via telnet or SSH, can you login and:**

- 1) Type **servget 6** (for HTTPS). Make sure it responds that HTTPS is enabled.
- 2) Type **rc-status** while trying to login to the browser (after typing its IP address into the Web browser). "Apache2" should be listed.

### 1) Reset password from front panel (resetpw command) if cant login to browser or cli

I had one customer update to v5.0.2 who couldn't login to browser with either his password or the default password. He reset the password back to default and got in.

Try this only if can't login to either browser or CLI (if can connect via telnet/ssh, password is OK),

**Note:** Starting in version ~~5.2.1~~ (~~Apr 2015~~) **resetpw also sets LDAP and Radius to "Disabled"** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026 Update- this change was inadvertently left out of the v5.2.1 release. It will need to be added in with the next release (5.3.0?)

When resetpw is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled after performing a resetpw.

Q help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?

**A Keith's response (23 May 17)** Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of 'admin123'.

Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn't change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.

### Not supported displayed (v4.8.1 and below only)

**Note:** With Archive Versions 4.8.1 and below installed, a minor bug causes "**Not Supported**" to be displayed in the LCD, even though the command did reset the password.

### A) Known condition after updating (observed with at least 5.0.2 update) – may need to delete and recreate the HTTPS certificate via CLI using defcert command

- HTTPS certificate may become corrupted.
- Use **rc-status** CLI command to see if HTTPS is "scheduled"
- **defcert** command deletes HTTPS certificate and recreates it. Accept the new certificate next time logging into the browser.

### B) Known issue (Apache won't start after updating to versions 5.1.2 or higher – new browser won't open. Classic interface works normally)

- Verify cookies are enabled on the PC (for example, Firefox in private browser mode disables cookies). Apparently the new browser requires cookies but doesn't tell you that they have to be enabled. If cookies are disabled, can still get to login screen, by the login shakes as if the wrong password was entered.

### C) Known issue (Apache won't start after updating to versions 5.0.0, 5.0.1 or 5.0.2)

- After updating to a newer version, the port state (up or down depending on whether or not a cable is connected) can now be detected by the system. Apache has a dependency that the port be "up" before it will start.
- We have seen a couple instances where the port reports its down, even though it's still responding to everything but the web browser. Apache sees the port is down and will not start because of this dependency.

**Note:** The response of the “**rc-status**” CLI command (SSH connection) can be used to confirm this known issue is the cause. (Refer to [Specific available CLI commands/API calls/ functions](#)) (Abbreviated display below).

Verify “**Apache2**” and “**Apache2-cert**” are both “**Started**” (not “**stopped**” or “**scheduled**”)

```
Spectracom NetClock 9483 Version 5.0.2
admin@Spectracom ~ $ rc-status
level: default
kts [ started ]
identify [ started ]
syslogd [ started ]
logd [ started ]
nbe-load [ started ]
net.eth0 [ started ]
net.eth1 [ inactive ]
net.eth2 [ inactive ]
net.eth3 [ inactive ]
netmount [ started ]
apache2-cert [ started ]
apache2 [ started ]
snmpd [ started ]
snmpsd [ started ]
ntp [ started ]
fcron [ started ]
fcrontab [ started ]
swpple [ started ]
swpdie [ started ]
xhite [ started ]
scast485d [ stopped ]
scast485alarmd [ stopped ]
notifyd [ started ]
xtalogs [ started ]
```

**Note:** can also use portstate CLI command to report if ports are up or down.

```
Spectracom spectracom # portstate
eth0=Up
eth1=Unplugged
eth2=Down
eth3=Unplugged
Spectracom spectracom #
```

**To resolve:** Reboot doesn't fix this issue. Have to either have an engineer remote in to hand-start Apache, or update to versions 5.1.2 or higher, which are removing the dependency that Apache won't start if the port is down. Note: In order to apply an update without the browser being available on any port, must use the CLI commands to perform the update, instead of using the web browser.

#### D) Known issue in version 4.8.9 and below (Memory leak): Apache Web browser no longer accessible, but can still ping, telnet, etc. still work

- Version 5.0.0 update fixes this issue (It DOES NOT need to be power cycled to restore access to the browser)

**Right after entering username and password, web browser displays: “ERROR: The web server encountered an unexpected error and failed to display the page you requested.”**

**ERROR:** The web server encountered an unexpected error and failed to display the page you requested.

- This issue is due to system memory leak in at least versions 4.8.9 and below (should be resolved with 4.8M and 4.8.9 with 4.8.M released in May 2013 but not cut-in. Version 5.0.0 expected to be cut-in June 2013).

(9/11/12 KW) versions 4.8.6 and below (as well as 4.8.7 and at least 4.8.8) apparently have a memory leak occurring when the units have been up for an extended amount of time. There isn't enough free memory available to run Apache.

With a Telnet or SSH session, perform/capture the results of a “**free**” (or “**free mem**”) command and an “**uptime**” command. Send the results to Engineering for their review.

**Note:** the command **free -m** reports the free memory in “MB” so it’s easier to decipher.

```
spectracom secureSync version 4.0.0
[spadmin@spectracom ~]# free
              total          used          free          shared        buffers         cached
Mem:          507648          143348          364300             0           18844           50804
-/+ buffers/cache:          73700          433948
Swap:           0              0              0
```

**Note: Per Dave Sohn (8 Mar 2013):** Apache needs about **100MB** or more of free memory to run. If “free” memory is below 100MB, the web browser won’t be available.

---

### 1. “Target machine actively refused it xxx.xxx.xxx.xxx:80”

**Example:**

```
[Fiddler] The socket connection to 10.2.100.176 failed.
ErrorCode: 10061.
No connection could be made because the target machine actively refused it 10.2.100.176:80
```

- “HTTP” is likely disabled in Services (*Management -> Network* page of new browser)
- SecureSync can’t be reached / in the process of booting-up or rebooting.
- Try adding **Error! Hyperlink reference not valid.** to the front of the IP address.
- Try pinging it
- Wait a couple of minutes and try again, especially if it was recently rebooted.

---

### 2. “Firefox can’t establish a connection to the server at xxx.xxx.xxx.xxx” or Internet Explorer reports “Unable to connect”

- “HTTPS” is likely disabled in Services (**Management -> Network** page of new browser)
- Will automatically redirect to an HTTP (unsecure) connection, if HTTP is enabled in Services.

---

#### A. Full CF card is another reason besides memory leak that the web browser may not be accessible

- Refer to Salesforce cases such as 11568
- SNMP, NTP statistics (versions 4.4.0 and below) and/or NTP logs can potentially fill the CF card to 100% capacity, which will prevent the web browser from being able to open.
- In the case of the SNMP log being full, the log was full of “Subcontainer” error messages.

**Note:** Refer to Mantis case 2343 (<http://cvsmantis.int.rolia.com/mantis/view.php?id=2343>)

**Note:** Refer to the SecureSync logs section for more information about this potential condition.

- (Versions 4.4.0 and below only) In the case of the NTP Statistics being full, Paul Myers found that versions 4.4.0 and below weren’t rotating out any of the NTP statistics. After several years, they can become so large that they fill the CF card.

**Note:** Because the clean command was not available in versions 4.4.0 and below, this command is not a temporary fix. Need to send a 4.3.2 CF card to swap in and then update to at least v4.5.0 to prevent it from happening again.

- In the case of the NTP log being full, the log was full of “NTP Buffer overflow” messages.
- Use the `df <enter>` or `df -h <enter>` CLI commands to see if the CF card is full.

Type “**df -h**” at the command prompt (note there is a space between the “f” and the “-h”)

```
spectracom NetClock 7183 version 1.0.0
[spadmin@Spectracom ~]$ df -k
Filesystem          1K-blocks      Used Available Use% Mounted on
/dev/hda1           985188      557808   377336   60% /
shm                 253824         0    253824    0% /dev/shm
[spadmin@Spectracom ~]$
```

**Example of a full CF card below (using the df command)**

```
[spadmin@stjhnblab-mr-ntp-001 log]$ df
Filesystem          1K-blocks      Used Available Use% Mounted on
/dev/hda1           985188      984516         0 100% /
shm                 253824         0    253824    0% /dev/shm
```

**Note:** Refer to the “du” command information further below if the card is nearly or completely full.

- If the SecureSync’s time is manually set backwards (such as for simulation), FCron stops rotating logs until “time catches back up” to the “correct” time. This can cause the logs to become very large during that time.

Update: this issue was reportedly fixed in the version 5.0.0 software update. Refer to Mantis case 2091 (<http://cvsmantis.int.rolia.com/mantis/view.php?id=2091>)



---

## du command (use if the CF card is quite or completely full)

- Refer to <http://www.cyberciti.biz/faq/how-do-i-find-the-largest-filesdirectories-on-a-linuxunixbsd-filesystem/>

**Note:** If the card is full or nearly full, to see the top 10 largest directories (and each file, in “MB) perform the following command:

`du -hsx * | sort -rh | head -10`<enter> (where the vertical line “pipe” is CTRL and the key under backspace)

```
spadmin@Spectracom ~ $ du -hsx * | sort -rh | head -10
8.5M  log
832K  customize
664K  default
300K  update
104K  mibs
68K   config
16K   xfer
8.0K  cert
4.0K  server.pem.old
4.0K  server.key.old
```

---

## glibc detected \*\*\* double free or corruption (!prev): 0x08053648

- glibc detected \*\*\* double free or corruption (!prev): 0x08053648 displayed at login prompt (shown below)
- Reported by Robert Farrell w/Verizon (26 Feb 2014)
- Archive version 4.8.9 with 1204-06 card installed
- Appears to be the memory leak issue that was addressed in the version 5.0.0 update.
- Fix: update to versions above 4.8.9.

```
Spectracom login: spadmin
*** glibc detected *** double free or corruption (!prev): 0x08053648 ***
Spectracom login:
```

### Paul Myers responded

This may be indicative of a memory problem possibly a memory leak or memory problem.

- Is the Front panel updating?
- Can they change the front panel screen operation?
- Can the user login to the Web UI?
- Can they login to the serial console?
- Can they login SSH?
- Can they FTP connect? (probably not)

If the web ui is down too, they probably need to reboot, and update their unit to 5.1.2!

---

## \*Internet Explorer not displaying the gear icons on the web pages

- Refer to Salesforce case 24808.
- The \* setup Icons will not appear on the **Home** Status page or other pages.

**Finding:** Internet Explorer was set to use "Trusted Sites" and that was blocking the web UI.

## Login Banners

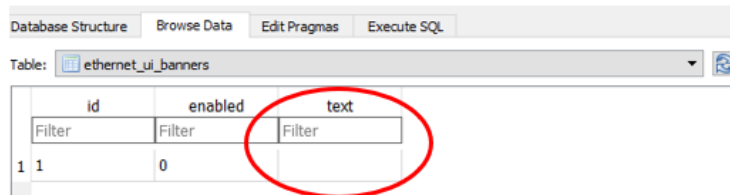
- login banners can optionally be displayed for **web browser login** and/or **CLI interface login**

### Storage of newer login banners (web browser and CLI interface)

- A) **CLI interface:** The login banner for the CLI interface is stored in the SecureSync's config files
- B) **Newer (black/charcoal) web browser:** The web browser login banner is not stored in the SecureSync's config files. Its instead stored in the sqlite database.

To view the browser's login banner, open the sqlite database, select the "**Browse Data**" tab and select the "**ethernet\_ui\_banners**" tables

1. With no web browser log banner created/stored (notice the "text" field is null/empty)

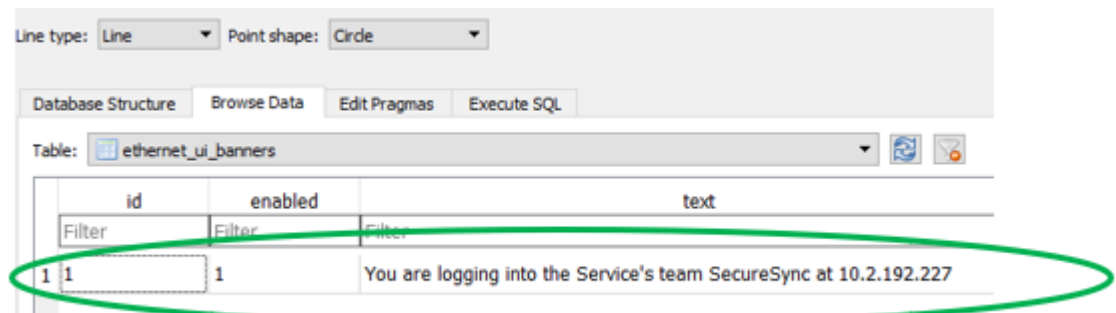
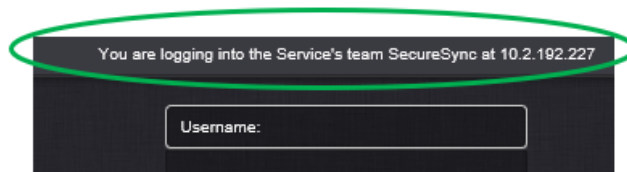


The screenshot shows a database browser interface with tabs for 'Database Structure', 'Browse Data', 'Edit Pragmas', and 'Execute SQL'. The 'Browse Data' tab is active, and the table 'ethernet\_ui\_banners' is selected. The table has three columns: 'id', 'enabled', and 'text'. The first row contains the values '1', '1', and an empty field. The 'text' field is circled in red.

| id | enabled | text |
|----|---------|------|
| 1  | 1       |      |

2. With web browser banner created/stored (placed in the "text" field)

*Sample web browser login banner was created*



The screenshot shows the same database browser interface as above, but the 'text' field in the first row now contains the banner text: "You are logging into the Service's team SecureSync at 10.2.192.227". The entire row is circled in green.

| id | enabled | text                                                               |
|----|---------|--------------------------------------------------------------------|
| 1  | 1       | You are logging into the Service's team SecureSync at 10.2.192.227 |

### Location of the browser login banner with the Config bundle

- The browser banner is stored in the **backup.sql.tar.gz** file (this file is also part of the extracted config bundle, in the home/spectracom/config directory)

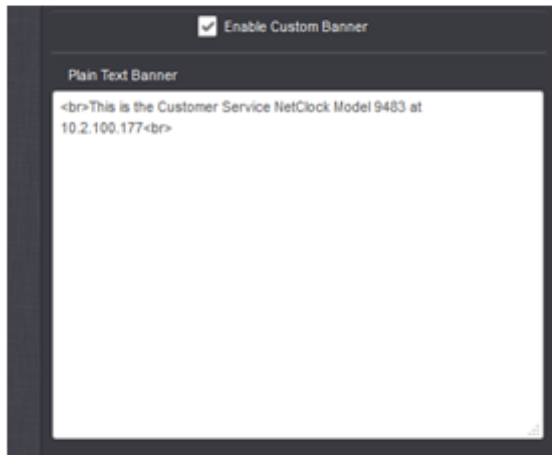
Home/spectracom/config/backup.sql.tar.gz file in the backup config bundle (screenshot from v5.8.5)



**Note:** The newer browser has two separate banners displayed/edited on this page. The top one is for telnet/ssh and the bottom one is for the web browser

Make sure the applicable “enable” button is selected if it’s desired to display the banner when logging in.

### Top banner (SSH login)



### Bottom banner (web browser login)



Sample Banner displays at bottom after pressing “Apply”

**Note:** “<br>” is to start a new line.

## B) Classic interface web browser

- The Banner configuration is in the *Network* -> *General Setup* page of the browser, Banner tab

**Note:** The classic interface only has one banner which is for the web browser.

Make sure the applicable “enable” button is selected if it’s desired to display the banner when logging in.

**Note about question below:** Question below was about the classic interface banner. Note sure it’s the same for the newer browser

Q. What is the maximum number of characters and lines allowed in the login banner (implemented in version 4.3.1 of the software)?

A. The login banner can be up to 2000 characters long. The number of available lines is not set to a specific number. But if the lines have significant numbers of characters, they won’t fit on the page.

As of 3/09/11 anyways, when created, the banner will display in all logins (web browser, ssh, telnet) with the exception of FTP. This is planned to be addressed in a post 4.4.0 software release.

## Desire for empty/white-space only lines between text lines

- Apparently, you can add hyphens to obtain blank lines.

Q. One minor issue I noticed - the Network Banner strips out empty or whitespace-only lines from what's pasted into the web form. I put in hyphens in order to get a line between paragraphs of the banner.

A. **Keith’s response:** Thanks for mentioning this to me. I spoke with our engineer who had implemented the banner capability in the software. He mentioned that code was implemented in the banner function to have this intentionally happen. He doesn’t recall the specific reasons he added it the code, but he found it was necessary while implementing this features. He believes it

may have been either associated with the window size on the login page, and/or many Carriage Returns would cause the banner text display to look “abnormal” with many lines of space being present.

---

## **Glibc**

- Update version 5.2.0 upgraded GLIBC package (in OpenSSL) from version 2.15 to 2.19 (addressing Ghost vulnerability, among other things).

---

## OpenSSL (Secure Socket Layer) /TLS-SSL for encryption (and HTTPD.conf file)/Security Level

### \*\*OpenSSL/TLS-SSL

- (Libraries for encryption)/ Ciphers for encryption

### SSL protocol versions (SSL versions 2.0 and 3.0)

- “OpenSSL version (Such as version 1.0.1k) isn’t the same as the “SSL protocol version (Such as SSL versions 2.0 or 3.0)
- SSL was replaced by TLS 1.0 after SSL version 3.0 (so there is no SSL version 4.0),
- In at least software versions v5.2.0 and above, SSL protocol versions 2.0 and 3.0 are disabled for both the newer and classic interface web browser (Both browsers only support TLS versions 1.0 and higher. They no longer support either SSLv2 or SSLv3).
- Paul Myers and Oleg confirmed that software version 5.0.2 had both SSL version 3 and TLS version 1 enabled (not SSLv2). SSL v3 was disabled sometime after v5.0.2 and by version 5.2.0 (Oleg believes it was around HeartBleed, like possibly v5.1.4/v5.1.5).
- See below for how to determine which SSL protocols are supported.

### \*\*\*TLS (Transport Layer Security) such as TLS 1.0, 1.1, 1.2 etc

- TLS is a “successor to SSL” (TLS was formerly known as “SSL”)
- SSL version 3.0 was the last version of SSL before TLS 1.0.

### TLS vs SSL

from <https://www.howmyssl.com/s/about.html>)

Okay, last thing. The jargon around is a little funny, so let's be a little more explicit. The 'S' in "HTTPS" is the TLS protocol. When folks refer to the "TLS" they are referring to the most common of modern protocols of encrypting data across the internet. "SSL", when used by experts, refers to the older versions of these protocols. In general, people use "SSL" and "TLS" interchangeably, but that's changing towards everyone saying "TLS". "TLS" is what everyone will call it in the future, while "SSL" is the phrase everyone knows right now.

### TLS protocol versions

- TLS protocol version 1.0 was first release of TLS, which replaced SSL v3
- TLS versions (such as versions 1.0, 1.1, 1.2 are protocols that can be enabled via the OpenSSL packages. It's not something that is automatically applied or automatically updated via an OpenSSL version update.
- See further below for how to determine which TLS protocols are supported.

### TLS 1.0 enabled / Desire to disable TLS (Enable High Security/“Hisec”)

(Ability to select both medium and high cipher OR just high/strong ciphers) (available in versions 5.4.5 and above)

### “SSL - Server Supports Weak SSL Ciphers”

- Ability to enable either ‘*both high and medium level ciphers*’, or ‘*high level ciphers only*’ was added in software version 5.4.5.
- Selecting the “Enable High Security” checkbox limits the ciphers list on the time server to only those algorithms considered most secure (preventing earlier browsers such as IE11 from being able to login)
- Factory default state is the “Enable High Security” checkbox NOT selected (providing both strong and medium ciphers for earlier browsers such as IE11 )

- Selection is in the **Management -> Network Setup** page of the browser (press the “**web interface settings**” button on the left). Then select the “Enable High Security” checkbox in the “Security Level” tab (as shown below):



Using the CLI interface (such as if browser is not accessible) to determine if “Enable High Security” is selected

To determine via CLI if “Enable High Security” is selected, type the following command: **cat /etc/apache2/services**

```
spadmin@Spectracom ~ $ cat /etc/apache2/services
```

- If the response lists both “USEHTTPS=”-D SSL” and **USEHTTPS=”-D HISEC”** (as shown below) the “Enable High Security” checkbox **IS** currently selected:

```
spadmin@Spectracom ~ $ cat /etc/apache2/services
USEHTTP=""-D HTTP"
USEHTTPS=""-D SSL"
USEHISEC=""-D HISEC"spadmin@Spectracom ~ $
```

- But if the response does not include “USEHTTPS=”-D HISEC” (as shown below) the “Enable High Security” checkbox **is not** currently selected:

```
spadmin@Spectracom ~ $ cat /etc/apache2/services
USEHTTP=""
USEHTTPS=""-D SSL"
spadmin@Spectracom ~ $ service 6 op
```

Security scan reported “**SSL/TLS server supports TLSv1.0 (“port 443/tcp over SSL)”**”

**Reply from Paul Myers (20 Dec 16)** TLS 1.0 is enabled for Medium level web browser security. High Security will disable TLS 1.0 at the cost of older browser support.

**How to verify which SSL and TLS protocols are enabled/disabled (can be performed with spadmin account)**

- 1) “**CD**” to the /etc/apache2/sites-enabled directory. Type (or copy/paste): **cd /etc/apache2/sites-enabled**
- 2) Type either:
  - (For newer browser): **cat 000-httpd-default.conf**

- (For classic interface browser): **cat 001-httpd-oldui.conf**
- 3) In each of these two conf files is an “**SSLProtocol**” line (like shown below and near the ciphers list). In this Example line, “ALL -SSLv2 -SSLv3” indicates all **TLS and SSL** protocols accept ssl 2.0 and ssl 3.0.
- **Note for TLS:** The word “**All**” includes all SSL and all **TLS** protocols. (not just “SSL”)

Example conf file entry for both the newer and classic interface browser, with version 5.2.0 software installed:  
**SSLProtocol ALL -SSLv2 -SSLv3** (“**All**” indicates all SSL and all TLS protocol versions)

**Example from v5.4.1 (showing in red that all versions of TLS - minus SSLv2 and SSLv3 - are currently enabled as of this release)**

```
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Security Patches
# CVE-2012-4929 CRIME attack on Gentoo BUG# 438680
SSLCompression off

# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+SSLv2:!EXP:!eNULL

SSLProtocol ALL -SSLv2 -SSLv3
SSLHonorCipherOrder On
#SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4-SHA:+HIGH:+MEDIUM
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-ge
```

---

## SSL Cipher suites (CBC Ciphers) / MAC Algorithms

- OpenSSL in the NTP servers have a supported Ciphers list. The client also has its own list of supported ciphers.
- The supported ciphers list is in order of most secure to least secure, with the considered most secure at the top of the list and the least secure at the bottom of the list
- The client and NTP server negotiate which cipher to use, typically the first common one in both lists. This allows the most secure cipher, supported by both Server and Client to be selected for encryption.

### **\*\*SHA-1(SHA1) vs SHA-2 (SHA2) family (SHA-224, SHA-256, SHA-384, SHA-512)**

- Refer to <http://www.infoworld.com/article/2879073/security/all-you-need-to-know-about-the-move-to-sha-2-encryption.html>
- “SHA-2, the set of cryptographic hash functions to succeed SHA-1”

## Intro to SHA

- SHA stands for (Secure Hash Algorithm) and were created by the NSA.
- The number after “SHA” is the hash value (number of bits).

SHA-1 was designed by the NSA and published as a federal standard in 1995. Hashes are used for digitally signing content for integrity validation and are a part of any digital certificate. Without cryptographically sound hashing algorithms, digital authentication and integrity would be very hard to do, if not impossible.

In 2002, SHA-2 became the new recommended hashing standard. SHA-2 is often called the SHA-2 family of hashes because it contains many different-size hashes, including 224-, 256-, 384-, and 512-bit digests. When someone says they are using the SHA-2 hash, you don’t know which bit length they are using, but the most popular one is 256 bits (by a large



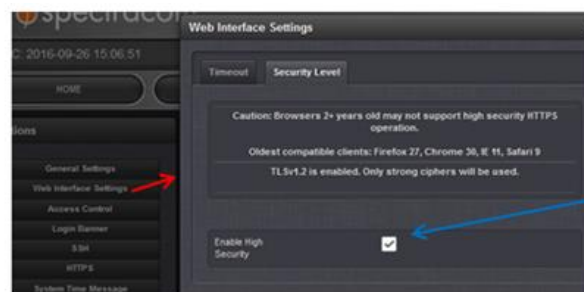
margin). Although SHA-2 is constantly attacked and minor weaknesses are noted, in crypto-speak, it's considered "strong." Without question, It's way better than SHA-1, which experts believe will be fallible in the near term.

## TLsv1.2 Security Level selection (HiSec/Enable High Security) (applicable to versions 5.4.5 and above)

Refer to the "**HTTPS Security Levels**" section of the online SecureSync user guide at:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/HTTPSsecurityLevel.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/HTTPSsecurityLevel.htm)

- Ability to select either high and medium level ciphers or just high level ciphers was added in software version 5.4.5.
- Update version 5.4.5 added the ability to either limit the newer black browser to use only strong security ciphers or to allow it to use both medium and strong ciphers (As determined by the requirements of the browsers desiring to connect to the SecureSync)
  - In v5.4.5 and above, there are now two different cipher lists. This checkbox determines which of the two is used).
  - TLSv1.2 is enabled when high Security is selected.
- Selecting "**Enable High Security**" limits the ciphers list to only those algorithms considered most secure.
- Selection is in the **Management** -> **Network Setup** page of the browser (press "**web interface settings**" button on the left). Then select the "**Enable High Security**" checkbox in the "Security Level" tab \*as shown below):



**To view the ciphers list for either the new browser or the classic interface (can be done with spadmin account) perform either of the following:**

- The first method (A below) just displays the list of all available cipher suites in the OpenSSL version installed (not which ones we support and don't support for various connections)
- The second method (B below) shows which ciphers are allowed and which ones are not allowed.

**A) To see all ciphers available in OpenSSL versions installed**

1. Login as spadmin and type **openssl ciphers** <enter>

```

Telnet 10.2.100.89
Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ openssl ciphers
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384
4:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDSA-AES256-SHA:SRP-DSS-
AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256
-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:DHE-RSA-AES256-SHA:DHE-D
SS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:ECDSA-AES256-GC
M-SHA384:ECDSA-AES256-GCM-SHA384:ECDSA-AES256-SHA384:ECDSA-AES256-SHA:ECDSA-AES256-S
HA384:ECDSA-AES256-SHA:ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:
AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA:ECDSA-AES256-CBC3-SHA:ECDSA-
DES-CBC3-SHA:SRP-DSS-3DES-EDE-CBC-SHA:SRP-RSA-3DES-EDE-CBC-SHA:EDH-RSA-DES-CBC3
-SHA:EDH-DSS-DES-CBC3-SHA:ECDSA-DES-CBC3-SHA:ECDSA-DES-CBC3-SHA:DES-CBC3
-SHA:PSK-3DES-EDE-CBC-SHA:ECDSA-AES128-GCM-SHA256:ECDSA-AES128-GCM-SHA
256:ECDSA-AES128-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:DHE-DSS-AES128
-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA25
6:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DHE-RS
A-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:ECDSA-AES128-GCM-SHA256:ECDSA-
AES128-GCM-SHA256:ECDSA-AES128-SHA256:ECDSA-AES128-SHA256:ECDSA-AES128-SHA:ECDSA-
AES128-SHA:ECDSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:SEED-SHA:
CAMELLIA128-SHA:IDEA-CBC-SHA:PSK-AES128-CBC-SHA:ECDSA-RC4-SHA:ECDSA-RC
4-SHA:ECDSA-RC4-SHA:ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:EDH-RSA-DE
S-CBC-SHA:EDH-DSS-DES-CBC-SHA:DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-EDH-DSS-DE
S-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:EXP-RC4-MD5
spadmin@Spectracom ~ $

```

B) To view the ciphers list allowed for either the new browser or the classic interface (can be done with spadmin account) perform either of the following:

1. Software versions 5.4.5 and above (v5.4.5 added ability to select either high or medium security).

**New black background browser**

- Refer to the process for versions 5.4.1 and below further down, if the classic interface is enabled and to display its list.

**Note:** This process below will only display the list for either High or Medium, depending on which is configured to be used. Screenshot below shows list for v5.4.5 with high security selected (instead of medium)

1. Type `cd /etc/apache2/sites-enabled` directory.
2. type the following: **vi 000-httpd-default.conf**
  - A. Press: `/` and then type **ssl** next to it
  - B. This will display the enabled and disabled SSL/TLS ciphers (Note that “ALL” includes SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, etc and ! before a cipher indicates not enabled).

**Note:** the “!” is a “not” symbol to exclude that item from being allowed

**Note:** to exit out of the file, press both `ctrl + z`

```
spadmin@spectracom ~ $ cd /etc/apache2/sites-enabled
spadmin@spectracom /etc/apache2/sites-enabled $ vi 000-httpd-default.conf
# CakePHP files: Basically if it isn't an existing file or dir, send it
# to cake's index.php
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ index.php [QSA,L]

# If client accepts compressed files and a compressed version exists,
# send that
RewriteCond %{HTTP:Accept-encoding} gzip
RewriteCond %{REQUEST_FILENAME}\.gz -s
RewriteRule ^(.*)\.css $1\.css\.gz [QSA]

# Serve gzip compressed JS files if they exist and the client
# accepts gzip.
RewriteCond %{HTTP:Accept-encoding} gzip
RewriteCond %{REQUEST_FILENAME}\.gz -s
RewriteRule ^(.*)\.js $1\.js\.gz [QSA]

# Serve correct content types, and prevent mod_deflate double gzip.
RewriteRule \.css\.gz$ - [I=text/css,E=no-gzip:1]
RewriteRule \.js\.gz$ - [I=text/javascript,E=no-gzip:1]

</Directory>

#
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Security Patches
# CVE-2012-4929 CRIME attack on Gentoo BUG# 438680
SSLCompression off

#
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+SSLv2:!EXP:!NULL
<IfDefine HISEC>
SSLProtocol ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
#SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+SHA:+HIGH:+MEDIUM
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-generator/?server=apache-2.2.31&openssl=1.0.2h&hsts=yes&profile=modern
# Tested with https://www.ssllabs.com/ssltest/analyze.html
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECHE-RSA-AES256-GCM-SHA384:ECHE-ECDSA-CHACHA20-POLY1305:ECHE-RSA-CHACHA20-POLY1305:ECHE-ECDSA-AES128-GCM-SHA256:ECHE-RSA-AES128-GCM-SHA256:ECHE-ECDSA-AES256-SHA384:ECHE-RSA-AES256-SHA384:ECHE-ECDSA-AES128-SHA256:ECHE-RSA-AES128-SHA256
</IfDefine>
```

```
<IfDefine HISEC>
SSLProtocol ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
#SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+SHA:+HIGH:+MEDIUM
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-generator/?server=apache-2.2.31&openssl=1.0.2h&hsts=yes&profile=modern
# Tested with https://www.ssllabs.com/ssltest/analyze.html
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECHE-RSA-AES256-GCM-SHA384:ECHE-ECDSA-CHACHA20-POLY1305:ECHE-RSA-CHACHA20-POLY1305:ECHE-ECDSA-AES128-GCM-SHA256:ECHE-RSA-AES128-GCM-SHA256:ECHE-ECDSA-AES256-SHA384:ECHE-RSA-AES256-SHA384:ECHE-ECDSA-AES128-SHA256:ECHE-RSA-AES128-SHA256
</IfDefine>

# This is essentially an else
<IfDefine !HISEC>
SSLProtocol ALL -SSLv2 -SSLv3
SSLHonorCipherOrder On
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-generator/?server=apache-2.2.31&openssl=1.0.2h&hsts=yes&profile=intermediate
# Tested with https://www.ssllabs.com/ssltest/analyze.html
```

```

SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-
GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-
AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-
RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:!ECDHE-ECDSA-DES-CBC3-
SHA:!ECDHE-RSA-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:!DES-CBC3-SHA:!DSS
</IfDefine>

```

## 2. Software Versions 5.4.1 and below - Perform the following to view the list in the ssl.conf file

1. CD to the `/etc/apache2/sites-enabled` directory.
2. Either:
  - (For ciphers allowed with newer browser) type the following: **vi 000-httpd-default.conf**
  - (For ciphers allowed with classic interface browser) type the following: **vi 001-httpd-oldui.conf**
3. press: `/` and then type **ssl** next to it
4. This will display the enabled and disabled SSL/TLS ciphers (Note that “ALL” includes SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, etc and `-SSLv2` and `-SSLv3` for example excludes SSLv2 and v3 ).

**Note:** the “!” is a “not” symbol to exclude that item from being allowed

**Note:** to exit out of the file, press both `ctrl + z`

```

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Security Patches
# CVE-2012-4929 CRIME attack on Gentoo BUG# 438680
SSLCompression off

# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+SSLv2:!EXP:!eNULL

SSLProtocol ALL -SSLv2 -SSLv3
SSLHonorCipherOrder On
#SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4-SHA:+HIGH:+MEDIUM
SSLCipherSuite DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:CAMELLIA256-SHA:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:CAMELLIA128-SHA:RC4-SHA:RC4-MD5:RC4-MD5

```

---

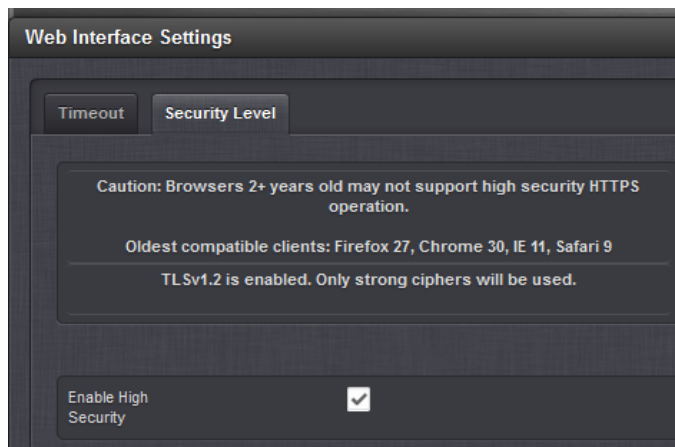
### Configure SecureSync to use High-level ciphers only

- I believe default is to allow both medium and high ciphers to be used
  1. Navigate to the **Management** -> **Network** page
  2. On the left side of the page, click “**Web interface Settings**”
  3. Select the **Security Level** tab.
  4. Select the “**Enable High Security**” checkbox to disable the medium-level security ciphers and press Submit.

### Medium and Strong security configured



### Enable High Security ciphers



### How is the cipher chosen in an SSL or TLS session?

- From <http://luxsci.com/blog/256-bit-aes-encryption-for-ssl-and-tls-maximal-security.html>

*In general, when an SSL client, such as an email program or web browser, connects to a server and wishes to use SSL or TLS, the client sends the server a list of encryption ciphers that it supports. The server then goes through the list, in order, and chooses the **first match** that it also supports. Usually, the client orders the list with the most secure methods first, so that the most secure method supported by both the client and server is selected. Sometimes, the client orders the list based on other criteria to make a compromise between security and speed; this can result in a sub-optimal cipher being chosen.*

*Most modern web and email servers that support SSL encryption, like LuxSci.com’s servers, support many different strong encryption techniques all the way up to 128-bit RC4 and 256-bit AES. They provide a variety, instead of just a single really good method, so that users who have old or broken software can still take advantage of encryption, even if it is weaker than it should be. Additionally, most companies that provide security services do not permit use of techniques that deemed are “too weak” and which can be broken very easily (like the old “[export grade ciphers](#)” that used to be in prevalent use). So, if you are connecting to a reputable service provided over SSL or TLS, the type of encryption that will be used is almost certainly determined by **your** client program (i.e. email program or web browser).*

Q. What is the maximum SSH cipher suites that the box can support?

A. As for the question on cipher suites, below is a screenshot of the SSH configuration page. This screen will likely answer many of your customer’s questions about SSH configuration of the SecureSync.

HTTPS SSH

### Host Keys

|                            |                       |
|----------------------------|-----------------------|
| Delete Host RSA Key File   | Enabled               |
| Delete Host DSA Key File   | Disabled              |
| Delete Host ECDSA Key File | Disabled              |
| Create Host Key Files      | Disabled              |
| Host Key Status            | Valid RSA, DSA, ECDSA |
| RSA Key Length             | 2048                  |
| DSA Key Length             | 1024                  |
| ECDSA Key Length           | 521                   |

### SSH Authentication

|                     |                        |
|---------------------|------------------------|
| Authentication Type | Public Key or Password |
|---------------------|------------------------|

### Public Keys File

|              |          |
|--------------|----------|
| View or Edit | Disabled |
|--------------|----------|

As shown in the screenshot above, SecureSync supports **RSA, DSA and ECDSA** encryption (as mentioned earlier, it does not support AES). The allowable key sizes for each of these algorithms are listed below:

- RSA keys can be 768 to 4096 bits
- DSA keys are limited to 1024 bits
- ECDSA keys can be 256, 384 or 521 bits

The SecureSync also supports Authentication of Password only, Public Key only, or either of these (as configured in the “Authentication Type” drop-down field).

## HTTPD.conf file

Q. Is there a way to look at the httpd.conf file?

A. **Per Dave Sohn (22 Apr 014)** httpd.conf is visible in the /etc/apache2 directory on the SecureSync. There are additional conf files in the /etc/apache2/sites-enabled directory

```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.4
spadmin@Spectracom ~ $ cd /etc/apache2
spadmin@Spectracom /etc/apache2 $ ls
httpd.conf magic modules.d services sites-enabled ssl.conf vhosts.d
spadmin@Spectracom /etc/apache2 $
spadmin@Spectracom /etc/apache2 $ ls
httpd.conf magic modules.d services sites-enabled ssl.conf vhosts.d
spadmin@Spectracom /etc/apache2 $ cat httpd.conf
# This is a modification of the default Apache 2.2 configuration file
# for Gentoo Linux.
```

```
spadmin@Spectracom /etc/apache2 $ cd sites-enabled
spadmin@Spectracom /etc/apache2/sites-enabled $ ls
000-httpd-default.conf 001-httpd-oldui.conf
spadmin@Spectracom /etc/apache2/sites-enabled $
```

## UserDir Disabled

Q. Can you confirm the following directive command is set in httpd.conf file for the SecureSync 1200 appliance? **"UserDir Disabled"** in httpd.conf file. This directive value is a fix for CVE2001-1013

**A. Per Dave Sohn (22 Apr 2014)** This directive command is not in SecureSync. However, no username disclosure is available via the SecureSync via the vulnerability described. When tested, all user directory queries respond with a 404 response whether the username exists on SecureSync or

---

## **\*\*AES (Advanced Encryption Standard)**

- AES is a specification for the encryption of electronic data.

Q. What BIT (size) of AES encryption is supported?

**A. Email from Paul Myers (2/2/12)** "We support "AES 128, 192, and 256 bit ciphers"

---

## **\*\*MTU (Maximum Transmission Unit)**

- for info on MTU: [http://en.wikipedia.org/wiki/Maximum\\_transmission\\_unit](http://en.wikipedia.org/wiki/Maximum_transmission_unit)
- In versions 5.1.4 and below, MTU is hard-set to 1500 (users cannot change)
- Harris requested ability to change this value to 1400. Refer to Salesforce case 13244.
- Ability to change MTU value was added in update version 5.1.4.

## \*\*Network ports/Management/Network Access restriction (Access control)

- **Internal use only**- for CLI, the access table entries are in /home/spectracom/config and type: `cat access.conf`

**Note:** refer also to “IPTables” (applicable to versions 5.4.0/5.4.1 and above) for customized port restriction capabilities.

**Important note:** entering a subnet value of “/0” is not valid. In versions 5.3.0 and below, it will cause Apache to crash and prevent access to the browser. In versions 5.3.0 and below, the browser doesn’t prevent a user from inadvertently entering this value (Refer to Mantis case 3110). This potential condition was fixed in **version 5.3.1**.

**Format of table entries:** uses **CIDR format** (x.x.x.x/zz (where zz is the two digit subnet mask. Example: 10.10.1.1/32)

The two digit subnet mask does not have to be the same mask that the network is using. With using CIDR in this particular functionality of blocking access, the specified address and the subnet are “or” together to determine a range of allowable addresses. So an even smaller subnet of allowed addresses can be defined, than the subnet that the time server is plugged into.

- If it’s desired to define one specific IP address (and allow no others on that same subnet), use the two digit subnet mask of /32. Note that more than one address using “/32” can be added to the list to allow access to more than one specific address.
- If it’s desired to allow access to any nodes that have the same last octet as the configured address, use a subnet mask of /24
- If it’s desired to allow access to any nodes that have the same last two octets as the configured address, use a subnet mask of /16.

**Note:** IP address(es) must be entered in CIDR format (“IP address / two digit subnet mask) as described further above.

To calculate the CIDR value to use, refer to online CIDR tools such as <https://www.subnet-calculator.com/cidr.php> (change the CIDR Netmask to the value which allows the number of individual PC’s desired, or to a value that allows the desired entire subnet)

**Note:** IP address(es) must be entered in CIDR format (“IP address / two digit subnet mask) as described further above.

- To limit access to only one PC for example: 10.10.128.2/32

| CIDR | SUBNET MASK     | WILDCARD MASK | # OF IP ADDRESSES | # OF USABLE IP ADDRESSES |
|------|-----------------|---------------|-------------------|--------------------------|
| /32  | 255.255.255.255 | 0.0.0.0       | 1                 | 1                        |

To limit access to only two PCs for example: 10.10.128.2/30

| CIDR | SUBNET MASK     | WILDCARD MASK | # OF IP ADDRESSES | # OF USABLE IP ADDRESSES |
|------|-----------------|---------------|-------------------|--------------------------|
| /30  | 255.255.255.252 | 0.0.0.3       | 4                 | 2                        |

- To limit access to an entire subnet of 255.255.255.0: 10.10.128.2/24

| CIDR | SUBNET MASK   | WILDCARD MASK | # OF IP ADDRESSES | # OF USABLE IP ADDRESSES |
|------|---------------|---------------|-------------------|--------------------------|
| /24  | 255.255.255.0 | 0.0.0.255     | 256               | 254                      |

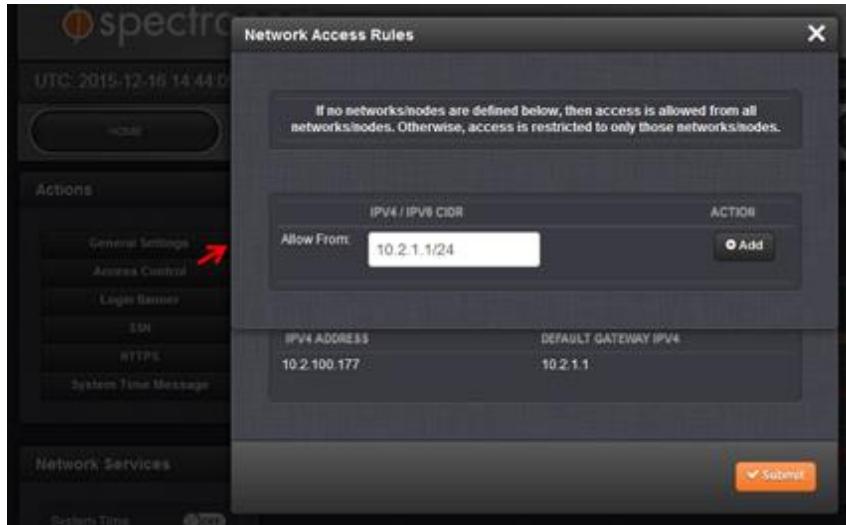
- To limit access to an entire subnet of 255.255.0.0: 10.10.128.2/16



| CIDR | SUBNET MASK | WILDCARD MASK | # OF IP ADDRESSES | # OF USABLE IP ADDRESSES |
|------|-------------|---------------|-------------------|--------------------------|
| /16  | 255.255.0.0 | 0.0.255.255   | 65,536            | 65,534                   |

### C) Newer black/Charcoal web browser:

*Management* -> *Network* page. Then click on “Access Control” (on the left side of the page)



### D) “classic interface” web browser

Network -> General Setup page, Access tab (as shown below)



### Command to reset the Network Access table (unrestrict)

Version 4.40 (possibly before) adds a new CLI command (“**unrestrict**”) to clear the Access table. In units with versions 4.5.0 or higher installed, no longer need to clean all configurations. This can be performed via the CLI- It’s not available via the keypad (it’s not in the front panel “Cmd” menu).

**Note:** the configs for network access restriction are stored in the **access.conf** file (**home/spectracom/conf** directory and then type: **cat access.conf**. If there is no response to this command, the table is empty (as shown below)

```

CustService-176 spectracom # cd config
CustService-176 config # cat access.conf
CustService-176 config #

```

Example from v5.3.1 showing no entries have been added to the Access table

```

spfactory@spectracom /home/spectracom $ cd config
spfactory@spectracom /home/spectracom/config $ cat access.conf
cat: access.conf: No such file or directory
spfactory@spectracom /home/spectracom/config $

```

Example from v5.3.1 showing an entry HAS been added to the table (type “*unrestrict*” to clear all entries in the table)

```

spfactory@spectracom /home/spectracom/config $
spfactory@spectracom /home/spectracom/config $ cat access.conf
10.2.100.124/16

```

---

## Access configuration storage

### A) Newer black/charcoal browser:

Access Restriction configuration is in the “access.conf” file (/config directory). The “access.conf” file is only present if Access Restriction configuration has been changed from the factory default settings.

```

spadmin@spectracom ~/config $ ls
access.conf  gpsrinexd.conf  notcf

```

After adding 10.2.0.0/16 to the Access Restriction page.

```

10.2.0.0/16
access.conf lines 1-1/1 (END)

```

**Important note (versions 5.3.0 and below):** entering a subnet value of “*0*” is not valid. It will cause Apache to crash and prevent access to the browser. In software versions 5.3.0 and below, the browser doesn’t prevent a user from inadvertently entering this value (Refer to Mantis case 3110). Version 5.3.1 update prevents the ability to accept this value.

### B) Classic interface browser:

Values entered in this Access Control table are stored in the /etc/apache2/httpd.conf file (example below from a file that has had values entered)

```

# NOTE: the following is updated programmatically by the system
# to implement access restrictions.
#
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Deny from all
    Allow from 172.16.0.0/12
    Allow from 10.0.0.0/8
    Allow from 192.168.60.0/24
    Allow from 100.100.100.0/23

```

```

Allow from 172.40.0.0/16
Allow from 192.168.40.2/24
Allow from 0.0.0.0/0 (note that "/0" is not valid and will cause Apache to crash (perform an unrestrict to
remove it)
Allow from 0.0.0.0/32
</Directory>

```

Base unit has one 10/100 Management port with Option Card (Model 1204-06) providing 10/100/1000 base-T network connections).

**Purpose of Management/Access:** Provides capability to restrict all management functionality (such as the web browser, telnet, FTP, etc) access to desired ports, with the exception of NTP

**Note:** Access applies to all network ports (Eth0, Eth1, Eth2 and Eth3)

**Note:** Version 4.40 (possibly before) adds a new CLI command ("**unrestrict**") to clear the Access table. In units with 4.5.0 or higher installed, no longer need to clean all configurations. This can be performed via the CLI- it's not available via the keypad (it's not in the front panel "Cmd" menu).

**Email from Dave Sohn (2 Apr 2013)** There is an error on the datasheet. There is no current mechanism to enable/disable management by individual ports. However, network access controls can be setup by IP address range to limit unit accessibility.

All network functionality including management and NTP is available from any interface.

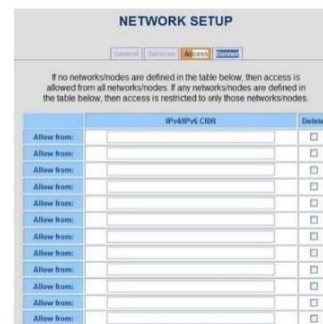
For your information, "Mgmt" (Management) is the ability to enable or disable all management services (such as HTTP/HTTPS/telnet, FTP, etc) from one or more of the SecureSync's Ethernet ports, thereby allowing only NTP functionality on that particular Ethernet port. It is primarily intended for those SecureSyncs with the available Gigabit multi-port Ethernet Option Cards (Model 1204-06) installed in the SecureSync. This Option Card adds an additional three network ports to the SecureSync (in addition to the standard base unit Ethernet port that is installed in every SecureSync).

The Management feature allows one or more network port/clients to be assigned SecureSync management capabilities, while all other network ports or PCs can only access the appliance via NTP. This available functionality is configured in the "Network"/"General Setup" page, "Access" tab, in the SecureSync's web browser. This functionality is also referred to as "Access Restriction" because it provides the means to block access to PCs that are not listed in this Access table.

By factory default and as long as the table in the "Access" tab remains empty, all network ports/clients are able to access the SecureSync, using any enabled service (as configured in the "Services" tab on this same page of the web browser). If a service is enabled in the Services Tab, and the Access tab has nothing configured in it, all port/clients can access SecureSync using that particular service (if a service is disabled, it's automatically not allowed on any network port).

The Ethernet ports themselves ("Eth0", "Eth1", "Eth2" and "Eth3") are not directly configured to restrict access by the port name/number. Instead, each port is indirectly restricted by its applicable IP addresses. For example, if the network connector "Eth1" is connected to a network with IP addresses of 192.168.1.x, if the 192.168.1.x network is not listed in the Access table (and if the Access table has any other values entered), the PCs that are connected to port "Eth1" will not have access to the management functions of SecureSync.

As shown in the left screenshot below, all of the "management services" are enabled (Daytime and Time protocols are not management protocols) and no clients or subnets have been configured to "allow" access via any of the management services (as shown in the right screenshot below), this indicates that any computer that can see this SecureSync can utilize any of the enabled services (assuming they know the login password, of course).



However, If its desired to prevent/block all services except NTP on a particular port or to most clients, you

configure the network address(es) that you want to allow all enabled services to be able to be accessed from, in the Access table. Then, if a network address is not listed in the Access tab, that network or particular PC will not have any access to SecureSync, other than NTP (it has to be listed to be able to access the SecureSync. The Access can be configured to allow an individual PC/client access or an entire subnet to have access to SecureSync.

To allow only specific IP addresses to have management capability, just list each desired IP address (that you wish to have management access) in individual "Allow From" fields. If a PC is not one of the configured IP addresses, it will not have management capability.

Configuring an entire subnet to have management capability uses CIDR notation (Classless Inter-Domain Routing) in each "Allow From" field. This format consists of the first IP address in the subnet, followed by a slash ("/"). The slash is then followed by a number representing the subnet mask. For more information on CIDR notation, refer to [http://en.wikipedia.org/wiki/CIDR\\_notation](http://en.wikipedia.org/wiki/CIDR_notation). Contact your network administrator to obtain the CIDR notation for the desired subnet, if you are not sure what this value should be.

An example of this CIDR formatting is: "192.168.0.0/24". If this example was to be added to an "Allow From" field in the Access table, the entire 192.168.0.0 network would then have management access. If it was the only entry listed in the Access table, the only computers that could then access the SecureSync would be the computers on the 192.168.0.0 network.

**Caution:** Entering an incorrect value in the Access table can potentially result in all network PCs being locked out of the SecureSync's web browser. If at least one undesired value is entered into the Access table and the configured value(s) do not correspond to the networks that are connected to SecureSync (none of the configured values in the Access table correlate to the networks that are connected to SecureSync), a PC will need to be directly connected to SecureSync (set the IP address of the stand-alone computer to a static IP address that was entered into the table. Otherwise, to regain access to the web browser, use the front panel CLI port to perform a "clean" (resets all of the SecureSync configurations back to the factory default values). **Note:** An automatic reboot is performed when performing a Clean command.

The following error message is displayed if the PC has restricted access to the SecureSync, because of the Access table configuration. ("You are trying to access a system file, which is forbidden...")

**ERROR:** You are trying to access a system file, which is forbidden. If you are linked to this file by the SecureSync product, please contact u

## **\*\*VLANs/VLAN tagging (IEEE 802.1Q)**

- Link to info on IEEE 802.1Q (regarding VLANS) [https://en.wikipedia.org/wiki/IEEE\\_802.1Q](https://en.wikipedia.org/wiki/IEEE_802.1Q)

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a **virtual local area network**, **virtual LAN** or **VLAN**.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical [local area network](#) (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same [network switch](#). VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

Portions of the network which are VLAN-aware (i.e., IEEE 802.1Q conformant) can include VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native (or

default) VLAN.

802.1Q does not encapsulate the original frame. Instead, for [Ethernet frames](#), it adds a 32-bit field between the source [MAC address](#) and the [EtherType/length](#) fields of the original frame, leaving the minimum frame size unchanged at 64 bytes (octets) and extending the maximum frame size from 1,518 bytes to 1,522 bytes (for the payload a 42-octet minimum applies when 802.1Q is present; when absent, a 46-octet minimum applies. IEEE 802.3-2005 Clause 3.5). Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, DEI, and VID.<sup>[3]</sup>

## ACS / AAA / Secure ACS (Cisco standards) protocols / environments.

Q. (From George Bown) Aimil our Indian partner are asking if SecureSync NTP server can work in ACS / AAA / Secure ACS ( Cisco standards) protocols / environments.

Reply from Keith (2 Feb 2015) Though the SecureSync supports its own network access restriction, I don't believe it supports Cisco AAA/ACS. It appears that special software is required to support this capability; I do know that the SecureSync has no special software installed to support it. So this is why I don't believe we support it.

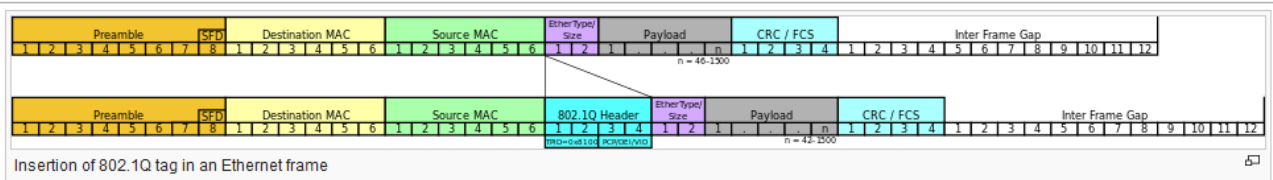
I have copied in Dave Sohn to confirm this, and also just so he is aware of the request to be able to support it.

FYI- Below is information regarding the SecureSync's/9400 series access restriction...

## VLANs/VLAN FRAMING/VLAN TAGGING

➤ Note info below is from [https://en.wikipedia.org/wiki/IEEE\\_802.1Q](https://en.wikipedia.org/wiki/IEEE_802.1Q)

### Frame format [\[edit\]](#)



802.1Q does not encapsulate the original frame. Instead, for [Ethernet frames](#), it adds a 32-bit field between the source [MAC address](#) and the [EtherType/length](#) fields of the original frame, leaving the minimum frame size unchanged at 64 bytes (octets) and extending the maximum frame size from 1,518 bytes to 1,522 bytes (for the payload a 42-octet minimum applies when 802.1Q is present; when absent, a 46-octet minimum applies. IEEE 802.3-2005 Clause 3.5). Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, DEI, and VID.<sup>[3]</sup>

|         |        |       |         |
|---------|--------|-------|---------|
| 16 bits | 3 bits | 1 bit | 12 bits |
| TPID    | TCI    |       |         |
|         | PCP    | DEI   | VID     |

- *Tag protocol identifier (TPID)*: a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType/length field in untagged frames, and is thus used to distinguish the frame from untagged frames.
- *Tag control information (TCI)*
  - *Priority code point (PCP)*: a 3-bit field which refers to the [IEEE 802.1p class of service](#) and maps to the frame priority level. Values in order of priority are: 1 (background), 0 (best effort), 2 (excellent effort), 3 (critical application), ..., 7 (network control). These values can be used to prioritize different classes of traffic (voice, video, data, etc.).
  - *Drop eligible indicator (DEI)*: a 1-bit field. (formerly CF)<sup>[note 1][4]</sup> May be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion.<sup>[5]</sup>
  - *VLAN identifier (VID)*: a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs. The reserved value 0x000 indicates that the frame does not carry a VLAN ID; in this case, the 802.1Q tag specifies only a priority and is referred to as a *priority tag*. On bridges, VID 0x001 (the default VLAN ID) is often reserved for a management VLAN; this is vendor-specific. The VID value 0xFFFF is reserved for implementation use; it must not be configured or transmitted. 0xFFFF can be used to indicate a wildcard match in management operations or filtering database entries.<sup>[6]</sup>

## VLAN tagged vs untagged

- Refer to sites such as <http://h30499.www3.hp.com/t5/Switches-Hubs-Modems-Legacy-ITRC/Tagged-vs-Untagged/td-p/4004330#.VbZ0hbWnTig>

### **Does SecureSync support VLANS (IEE 802.1Q)?**

- As of at least software version 5.8.2 and below, SecureSync does nothing specific to support VLANS (it is a “non-compliant 802.1 Q device”).
- VLAN routing is handled by the switch that the SecureSync is plugged into
- The SecureSync should be connected to an “**untagged**” port on a VLAN switch.

From: <http://www.microhowto.info/tutorials/802.1q.html#idp132208>

#### **Trunk and access ports**

*There are two ways in which a machine can be connected to a switch carrying 802.1Q VLAN traffic:*

- via an access port, where VLAN support is handled by the switch (so the machine sees ordinary, untagged Ethernet frames); or
- a trunk port, where VLAN support is handled by the attached machine (which sees 802.1Q-tagged Ethernet frames).

*It is also possible to operate a switch port in a hybrid mode, where it acts as an access port for one VLAN and a trunk port for others (so the attached Ethernet segment carries a mixture of tagged and untagged frames). This is not recommended due to the potential for VLAN hopping (described below).*

#### **Email from Dave Sohn about VLANS**

We don't provide any configuration capability to support VLAN-tagging directly on our interfaces. Customer edge switches can still be used to add VLAN tags to traffic from our units as it enters the connected switch ports to support their network needs. Do you have any more information on the customer's application?

#### **Good “draft” Email Keith sent to Ben Cosstick regarding whether SecureSync supports VLANS (27 Jul 2015)**

I am by no means an expert with VLANS. But with Dave Sohn out of the office, I'll give you my input on this.

VLAN tagging consists of tags (“frames”) added to standard network packets to direct the packets on trunk links to only certain parts of the network, as handled by the switches. For example, tags (frames) can be applied to only the packets that are intended for the “Engineering Dept”.

The SecureSync does not support the addition of VLAN tags/frames to its packets received or transmitted, so the switches outside of the SecureSync decide where to send the traffic on the network based on the destination address (no different than any other network). The switch port that the SecureSync connects to (an untagged port on the switch) strips the framing from all packets that are sent to the SecureSync. So the SecureSync receives a standard packet (no frames) from its switch. If it receives an NTP request from any VLAN, it simply responds to the address that sent the request to the time server. Its switch then routes the packet as necessary.

Because the SecureSync receives packets stripped of the VLAN tags, it can operate with as many VLANS that it can be routed to (the limit has nothing to do with VLANS and their tagging- the limit is based on how many VLANS it can physically get to through the network).

So, in summary, as far as the SecureSync is concerned (because it only processes packets stripped of their framing), there is no difference between syncing VLANS and syncing any other network.

Q We also like the multi-port GB module which we hope would allow us to have the timing system on multiple VLANS. Is it possible to run multiple instances of the NTP server on the SecureSync such that different servers can be accessed via different VLANS and ports? We believe this could provide us great benefit within our network architecture design.

A The Gb Ethernet card allows connection to up to 4 different subnets. VLANS are not directly supported via the SecureSync, however, the edge switches the SecureSync connects to can be set up with the appropriate VLANS for your network topology.

## Radius (Remote Authentication Dial-In User Service)

- Refer to sites such as <https://en.wikipedia.org/wiki/RADIUS>
- Refer to the SecureSync <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\LDAP and Radius>

### Tech notes available for Radius/LDAP

- **SecureSync LDAP / Radius tech note:** <EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\LDAP and Radius>
- **Model 9400 LDAP / Radius tech note** <EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\LDAP and Radius>

**RADIUS RFCs (in this document):** [\\*\\*Port assignments and RFCs for all products](#)

**OpenRadius:** <http://sites.e-advises.nl/openradius/>

**Shortcut to SecureSync LDAP/Radius design info:** <S:\Projects\Lafayette>

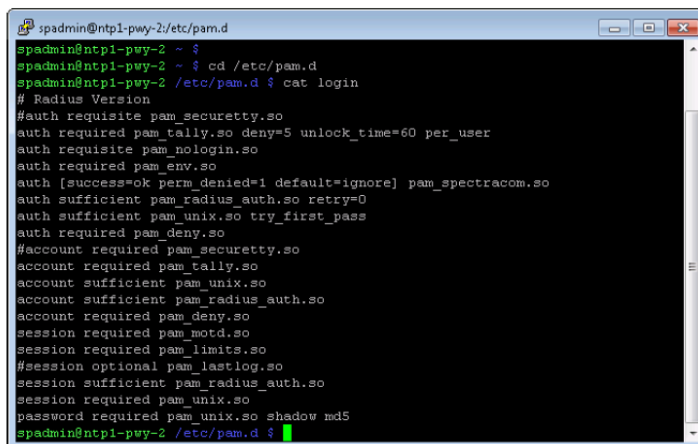
### Radius

**Note:** For example engineering software release testing of Radius, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 [https://app.bom.com/changes/detail-summary?change\\_id=2389346979](https://app.bom.com/changes/detail-summary?change_id=2389346979)) to find the PVP Test validation in the list of "ITEMS"

### Order of precedence for both Radius and LDAP when logging in (Per Ron)

- Radius authentication is attempted
- LDAP authentication is attempted.
- Local login (accounts in the NTP server).

As indicated: (internal use only) Spectracom/etc/pam.d/radius and type: **cat login**



```
spadmin@ntp1-pwy-2:/etc/pam.d
spadmin@ntp1-pwy-2 ~ $
spadmin@ntp1-pwy-2 ~ $ cd /etc/pam.d
spadmin@ntp1-pwy-2 /etc/pam.d $ cat login
# Radius Version
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth [success=ok perm_denied=1 default=ignore] pam_spectracom.so
auth sufficient pam_radius_auth.so retry=0
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
#account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account sufficient pam_radius_auth.so
account required pam_deny.so
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session sufficient pam_radius_auth.so
session required pam_unix.so
password required pam_unix.so shadow md5
spadmin@ntp1-pwy-2 /etc/pam.d $
```

### \*\*\*Our Radius server in Rochester

Set up and maintained by the IT team

**Note:** For example engineering software release testing of Radius, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.8.2 [https://app.bom.com/items/detail-spec?item\\_id=1208385170&version\\_id=11134640028&](https://app.bom.com/items/detail-spec?item_id=1208385170&version_id=11134640028&) ) to find the PVP Test validation in the list of "ITEMS"

For testing, a server with an IP address of **10.10.30.10**

**(IMPORTANT NOTE:** ping this address before changing our added to make sure engineering is not currently using it for their Radius/ldap testing)

**Note:** SecureSync has to be configured for a specific static IP address to work- [10.2.192.226](https://10.2.192.226) or [10.2.192.226](https://10.2.192.226)

**Management -> Authentication page and click Radius**

**Check the "HTTP/HTTPS" box**

**Retransmit attempts= 3**

**Host= 10.10.241.249**

**Port= 1812**

**Radius Secret key: 7cqptkHwjuGnvrL**

**Timeout = 10**

Click **"Add Server"**

**Login info**

**Username: dsohn**

**password: nsstest** (all lowercase)



---

## General info on Radius

### \*\*\*Radius Authentication versus Radius accounting

- Radius authentication (RFC 2865) provides remote authentication for connections (this is what we support)
- Radius accounting (RFC 2866) is often used for billing purpose

RADIUS accounting consists of an accounting server and accounting clients (PortMasters). The radiusd daemon for accounting is a child process of the radiusd authentication daemon; it starts automatically when radiusd is executed.

---

### Radius authentication messages

A RADIUS message consists of a RADIUS header and zero or more RADIUS attributes. Each RADIUS attribute specifies a piece of information about the connection attempt. For example, there are RADIUS attributes for the user name, the user password, the type of service requested by the user, and the IP address of the access server. RADIUS attributes are used to convey information between RADIUS clients, RADIUS proxies, and RADIUS servers

**Note:** For additional info on attributes, refer to: [https://en.wikipedia.org/wiki/Radius\\_Values](https://en.wikipedia.org/wiki/Radius_Values)

- **Access-Request**  
Sent by a RADIUS client to request authentication and authorization for a connection attempt.
- **Access-Accept**  
Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is authenticated and authorized.
- **Access-Reject**  
Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is rejected. A RADIUS server sends this message if either the credentials are not authentic or the connection attempt is not authorized.
- **Access-Challenge**  
Sent by a RADIUS server in response to an Access-Request message. This message is a challenge to the RADIUS client that requires a response.

---

### UDP Port 1813 (Radius accounting/ accounting messages)

- RADIUS accounting logs information about dial-in connections. This information is often used for billing purposes.
- With our Radius client configured to use port 1812, there are no messages sent/received on port 1813 (using tcpdump).

---

## Radius authentication

### Radius Extensions for OpenRadius (RFC 2869)

Extensible Authentication Protocol (EAP / (EAP-Message and Message-Authenticator)

Refer to RFC 2869 [http://datatracker.ietf.org/doc/rfc2869/?include\\_text=1](http://datatracker.ietf.org/doc/rfc2869/?include_text=1) (excerpt below)

The Extensible Authentication Protocol (EAP), provides a standard mechanism for support of additional authentication methods within PPP. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others. In order to provide for support of EAP within RADIUS, two new attributes, **EAP-Message** and **Message-Authenticator**, are introduced.

**FreeRadius support of EAP/** Refer to <http://freeradius.org/features/eap.html>

**FreeRadius Message Authenticator attribute:** <http://freeradius.org/rfc/rfc2869.html#Message-Authenticator>

**Radius Attributes:** RADIUS Attributes carry the specific authentication, authorization, information and configuration details for the request and reply.

Attributes defined in RFC 2869 include "User-Name", "Vendor-specific", "CHAP-Challenge", "framed", "Login", "NAS" and several others. Refer to **Section 5** at <http://freeradius.org/rfc/rfc2869.html#Message-Authenticator> )

---

## **\*\*Radius with IPv6 addresses**

**Mantis case 1722:** No current support for IPV6 Radius

- Applicable to at least versions 5.2.0 and below

**Update to this case (4 Apr 2013) Per Dave Sohn:** The pam\_auth\_radius module we use does not support IPv6. There is an IPv6 patch for it that would need to be tested. So the answer is we do not support IPv6 RADIUS at this time.

(3/23/11) Software versions 4.4.0 and earlier, LDAP and Radius authentication only work with the web browser login. Neither LDAP nor Radius worked with the other login services (SSH, telnet, etc). Unlike NetClock, no local user account needs to be created in the box to use LDAP or Radius.

With software version 4.5.0, we're adding LDAP authentication to all login services. However, Radius login is still restricted to just the web browser login. The other services (telnet, ssh, etc) will still require logging into a local account stored on the box, as we can't make Radius login available on the other login services.

Archive Version 4.8.0 removed the enabling of Radius with the CLI interfaces.

**Note:** SecureSync requires commas "," as separators between values. It can't accept periods "." as separators.

**Email from Dave Sohn 11/21- regarding Radius w/web browser only:** RADIUS is only utilized for authentication for HTTP/HTTPS because of a limitation at the time with the security package we were using for managing logins to the system. The RADIUS plugin only allowed it to be used for authentication against HTTP/HTTPS. RADIUS is probably low on the list for resolving issues, when looking at its usage and our resource utilization.

---

## **Notes about the need for User accounts and passwords being created/stored in SecureSync**

### **A) LDAP only**

Unlike earlier 9200 and 9300 series NetClocks, no User accounts have to be created in the SecureSync in order to use LDAP.

### **B) Radius only**

Unlike earlier 9200 and 9300 series NetClocks, no User accounts have to be created in the SecureSync in order to use Radius with the web browser (HTTP/HTTPS). However, due to technical limitations, Radius user can only login via the Web browser! Other services such as telnet and SSH are not technically available via Radius.

---

## **RSA authentication (SecurID)**

Unlike with the Model 9200 and 9300 series NetClocks, RSA authentication (SecurID) should be compatible with SecureSync/9400 series NetClocks. However, if a customer has any problems while using RSA authentication, please let Engineering know. See Mike Sander's comments below about this.

### **Email from Mike Sander**

I'm doing the SecureSync Radius app-note and I found the part about:

"RSA authentication requires a different Radius login password be entered when navigating from one page of the web browser to another. Radius requires the password to be the same value when navigating between pages of the browser. Using RSA authentication in conjunction with Radius will result in messages indicating the "password has been changed" being displayed when navigating in the time servers web browser. "

This may not be a problem with SecureSync. NetClock uses the Basic Auth type of Apache web authentication where the password is sent for every web page. We switched to an authentication module called Pamacea. Pamacea uses session files

to authenticate across web pages. So the web browser wouldn't be asking RSA for the password every time a page is displayed.

If enough customers ask about RSA we could try it again, maybe it works with Pamacea.

---

## Defining the LDAP/Radius account login permissions (user or admin)

Unlike earlier NetClocks, the SecureSyncs and 9400s don't need a user account created in the box. So there is no longer a place to configure whether the account has admin or user rights in the NTP server itself. For these units, this needs to be configured in the LDAP or Radius server.

### A) LDAP account permissions

For **LDAP**, refer to: "**Specific LDAP Server Configuration**" in the LDAP section of the Radius/LDAP Tech note in the SecureSync folder (pasted below, as well)

#### Specific LDAP Server Configuration

Follow the instructions specific to your LDAP server(s) to create and modify users in the LDAP server(s).

A SecureSync LDAP user needs the following LDAP fields:

|                  |                                                                        |
|------------------|------------------------------------------------------------------------|
| homeDirectory    | /home/spectracom                                                       |
| loginShell       | /bin/bash                                                              |
| uid              | A user name, (not "spadmin")                                           |
| uidNumber        | Use a number outside the range 1000 to 1050                            |
| <b>gidNumber</b> | <b>"admin" group is "111", "user" group is "112" (See Notes below)</b> |
| userPassword     | <password>                                                             |

#### **gidNumber attribute (used for SecureSync's CLI interface only- not used for web browser access)**

**Note:** "gidNumber" defines the permissions for each account, to be either **admin** account or **user** account. But only the **CLI interface** cares about this value. The web browser doesn't care, so LDAP users will be able to still use the browser, whether or not this attribute is assigned. But the CLI interface will not be accessible if this value is not assigned.

**Note:** The gidNumber is only used for access to **SecureSync's CLI interface** (such as telnet/SSH sessions). If the GID is not assigned as either of these two values, LDAP users won't be able to access CLI connections, but they **will still be able to access/use the web browser**, with admin rights. If scripting is desired to be used, the available REST API interface can be used, in lieu of logging into the SecureSync's dedicated CLI interface.

#### **(Case 186110): customer doesn't want to assign gidNumber 111 or 112 to all his AD accounts**

**email from Ron Dries, after checking with Stuart (20 Feb 2019)** The web UI should allow them to login without the gid set. All of the status and configuration they need can be done through the UI. If they need to script things they can use the REST API.

**Keiths response to this customer (20 Feb 2019) based on the response above from Ron** Note for your reference, I had assigned our Support case number 186110 to your questions. I apologize for the delay in being able to respond back to you, as I needed to first clarify a couple points with our Engineering team.

With some input from our Engineers, attached you should find a slightly revised copy of the SecureSync LDAP/Radius tech note you had mentioned referring to. I have updated the gidNumber info on page 14 of this document.

Specific to your questions/concerns of needing to hard-assign one of the two gidNumber attributes to your AD accounts, I found out that not performing this task results in only one very minor limitation (the CLI interface won't be accessible to the AD users).

The gidNumber attribute only applies to the SecureSync's CLI interface (such as telnet/ssh/ftp/scp connections). The CLI interface needs this attribute to be defined correctly, in order for the users' permissions to be provided by the AD server (unlike "local" accounts, such as the spadmin account, which have these permissions defined/stored inside the SecureSync itself).

However, the SecureSync's web browser doesn't utilize the gidNumber attribute. If an LDAP user has been authorized by AD to access the SecureSync, that user will automatically have permission to access/use the browser interface. It doesn't matter to the browser if this attribute is set to 111,112, or any other value.

As the browser provides the ability to perform all configurations of the SecureSync, not defining the gidNumber (thereby, only preventing access to the CLI interface, but not the browser) provides no configuration limitations. And if by chance its desired for AD accounts to be able to perform scripting, the available REST API (having the same permissions as the web browser) can be used to perform this task, in lieu of having access to the dedicated CLI interface.

Please let us know if you would like additional information pertaining to the availability of the REST API interface for the browser.

### Active directory permissions (user or admin)

Q. The instructions to setup different permissions levels, that is shown below, doesn't make sense to me. I can not setup a "gidNumber" with my active directory. Maybe these instructions are more Linux based machines? How do I do this is active directory? I will attach a screenshot of all the attributes of a user on my active directory.

A **Email from Dave Sohn (19 Mar 2013)** "Below is my best effort. I can't guarantee all of this, but I believe this is all accurate."

I believe the information that is requested for the Specific LDAP Server Configuration is independent of Linux or Windows. This needs to be present on both. If the user completes authentication, but an object like the Group ID is missing, then they will default to user privileges. I don't have a Windows Server 2008 installation to look at, but on the Windows Server 2003 I can see these. They need to enable editing/display of UNIX attributes, which means the schema of their Active Directory installation needs to be extended. They should have installed "Identity Management for UNIX" role service installed. You should now see a tab labeled "UNIX Attributes" in the properties for users and groups. The group ID of the domain group used to collect users for the SecureSync management needs to be set to **111 or 112** depending on admin or user privileges. Then for each of the users, you need to setup their UNIX attributes as described and make them a member of that group within the UNIX attributes.

### B) Radius account permissions

(8/24/12 KW) For **Radius**, accounts, I'm not sure at this time on how this is defined in the radius server. But since the User accounts don't have to be in the NTP server, it has to be defined somehow in the Radius server itself, similar to how it's done with LDAP.

**Note:** Information below is not yet confirmed to be correct (but may work). I haven't added this to the LDAP/Radius document yet- waiting on some feedback as to if this info is correct. Then, it should be added.

(8/29/12 KW email I sent to Jeremy Halterman with Harris)  
As for a FreeRadius Server (a Radius server running open source FreeRadius program), I found the following at <http://kb.juniper.net/InfoCenter/index?page=content&id=KB19446&actp=RSS>.

It looks like the "Service-Type" (bolded and enlarged below) may define the Login permissions. Login should be defined as "Admin". Refer to this website page for the full context of this information.

RADIUS server configuration:

In this example a freeradius server is used (more info about freeradius at <http://freeradius.org/>). The following users are configured in the file `/etc/freeradius/users` on the freeradius server:

```
tom Cleartext-Password := "tom123"
Service-Type = Login-User,
Juniper-Local-User-Name := "readonly-users",

jerry Cleartext-Password := "jerry123"
Service-Type = Login-User,
Juniper-Local-User-Name := "super-users",
```

This may work with a FreeRadius Server. If the Radius server isn't running open source software, you may need to contact the Radius server vendor to find out how to edit user account permissions.

---

#### \*\*\*\*Windows Active Directory / Radius Server / Group policy / Radius clients

**Refer to:** <http://technet.microsoft.com/en-us/library/dd759205.aspx> (Info for Server 2003, Server 2008. Server 2012)

**Radius Client:** <http://technet.microsoft.com/en-us/library/cc754033.aspx>

---

#### \*\*\*Radius vendor-specific attributes (vendor specific attributes) (VSAs)-Vendor code/Vendor ID

- Refer to Salesforce case 12223
- Refer to <https://en.wikipedia.org/wiki/RADIUS>

RADIUS is extensible; many vendors of RADIUS hardware and software implement their own variants using Vendor-Specific Attributes (VSAs).

##### Vendor specific attributes

In addition to the RADIUS standard attributes, which are described in Request for Comments (RFC) 2865 and RFC 2866, you can configure vendor-specific attributes (VSAs) in Network Policy Server (NPS) network policy and connection request policy that are returned to RADIUS clients in RADIUS response messages.

VSAs allow RADIUS client vendors, such as the manufacturers of wireless access points, 802.1X authenticating switches, and devices that act as virtual private network (VPN) servers, to support their own proprietary RADIUS attributes that are not included in the RFCs. NPS includes VSAs from a number of vendors in its dictionary; however, the NPS dictionary does not include VSAs for all vendors.

Some network access server (NAS) manufacturers use VSAs to provide functionality that is not supported in RADIUS standard attributes. NPS enables you to create or edit VSAs to take advantage of proprietary functionality supported by some NAS vendors.

##### Service-Type attribute Email from a customer

Thanks for looking into to it for us. We are using Microsoft NPS as our RADIUS. I tried configuring (service-type – Administrative) on the Microsoft side. It looks like it gets sent back to SecureSync with the accept-accept packet, though it has no effect. Not sure if you guys use any vendor specific Attribute-value pairs or not. Our next go was to look at the pam\_auth\_module that SecureSync uses.

**Email from Dave Sohn (28 Oct 2013):** I'm not sure that we have any vendor specific attributes, or a vendor ID. See more info here on VSAs. [http://technet.microsoft.com/en-us/library/cc754417\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754417(v=ws.10).aspx) (excerpt below):

Q. We are using Microsoft NPS as our RADIUS. I tried configuring (service-type – Administrative) on the Microsoft side. It looks like it gets sent back to SecureSync with the accept-accept packet, though it has no effect.

Not sure if you guys use any vendor specific Attribute-value pairs or not. Our next go was to look at the pam\_auth\_module that SecureSync uses.

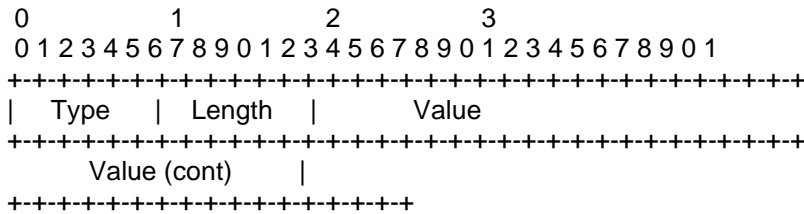
#### From RFC 2865

##### Description

This Attribute indicates the type of service the user has requested, or the type of service to be provided. It MAY be used in both Access-Request and Access-Accept packets. A NAS is not required to implement all of these service types, and MUST treat unknown or unsupported Service-Types as though an Access-Reject had been received

instead.

A summary of the Service-Type Attribute format is shown below. The fields are transmitted from left to right.



Type 6 for Service-Type.

Length 6

The service types are defined as follows when used in an Access- Accept. When used in an Access-Request, they MAY be considered to be a hint to the RADIUS server that the NAS has reason to believe the user would prefer the kind of service indicated, but the server is not required to honor the hint.

**Login** The user should be connected to a host.

**Framed** A Framed Protocol should be started for the User, such as PPP or SLIP.

**Callback Login** The user should be disconnected and called back, then connected to a host.

**Callback Framed** The user should be disconnected and called back, then a Framed Protocol should be started

for the User, such as PPP or SLIP.

**Outbound** The user should be granted access to outgoing devices.

**Administrative** The user should be granted access to the administrative interface to the NAS from which privileged commands can be executed.

**NAS Prompt** The user should be provided a command prompt on the NAS from which non-privileged commands can be executed

**Authenticate Only** Only Authentication is requested, and no authorization information needs to be returned in the Access-Accept (typically used by proxy servers rather than the NAS itself).

**Callback NAS Prompt** The user should be disconnected and called back, then provided a command prompt on the NAS from which non-privileged commands can be executed.

**Call Check:** Used by the NAS in an Access-Request packet to indicate that a call is being received and that the RADIUS server should send back an Access-Accept to answer the call, or an Access-Reject to not accept the call. Typically based on the Called-Station-Id or Calling-Station-Id attributes.

---

## 802.1x authentication (Encapsulation of EAP – also called EAPOL)

- As of at least software versions 5.1.4 and below, SecureSync does not support 802.1x
- It's a part of freeradius, but we don't have the Supplicant application software to support it.
- Radius server handles the certificates –SecureSync is just a supplicant.
- SecureSync would need third-party application software installed to make it a Supplicant. Refer to the following link for good info on this software:

[http://www.nowiressecurity.com/articles/third-party\\_80211x\\_client\\_supplicant.htm](http://www.nowiressecurity.com/articles/third-party_80211x_client_supplicant.htm)

From Wikipedia ([http://en.wikipedia.org/wiki/IEEE\\_802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X))

IEEE 802.1X is an [IEEE Standard](#) for port-based [Network Access Control](#) (PNAC). It is part of the [IEEE 802.1](#) group of networking protocols. It provides an [authentication](#) mechanism to devices wishing to attach to a [LAN](#) or [WLAN](#).

Requires both Radius and EAP ([http://en.wikipedia.org/wiki/Extensible\\_Authentication\\_Protocol](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol))

IEEE 802.1X defines the encapsulation of the [Extensible Authentication Protocol](#) (EAP) over [IEEE 802<sup>1/2</sup>](#) which is known as "EAP over LAN" or EAPOL

With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network

Q. Do we support 802.1x authentication?

**A. Email from Ron Dries (8 July 2014) referring to at least version 5.1.4 software**

FreeRadius does support 802.1x but the configuration for that is at the server level not the client. The Radius authentication server gets configured for 802.1x and generates the certificates.

However the SecureSync is not the authentication server, but a client. It appears in the 802.1x standard the SecureSync would be considered a supplicant, a device that requires authentication. For this it would need a supplicant application, i.e. Xsupplicant, installed and would need to be configured correctly for 802.1x.

So currently we do not support this feature, because we do not have the ability to make the SecureSync a supplicant.

I hope I was able to answer your question, if you have any further questions please let me know.

**A. older Email from Mike Sander (2/2/12)**

We don't support 802.1x authentication. It can be added to RADIUS, but we don't currently support it. It looks like a significant effort, adding packages to Linux, and supporting a new kind of certificate.

### \*\*\*Radius configuration

- **online SecureSync user guide:**  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/RADIUS\\_Auth.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/RADIUS_Auth.htm)

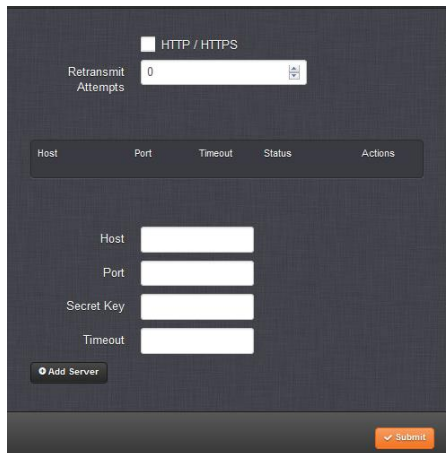
#### A) Configuration via CLI interface commands

- Not sure which software version these were added in (possibly v5.1.7??)
- Type **radius** <enter> to view the list of all radius commands

```
spadmin@Custservice177 ~ $ radius config
Radius command usage:
radius setretry <value>                : set retry value
radius getretry                         : shows retry value
radius server list                       : list servers by <id>
radius server add <host> <port> <key> <timeout> : add server
radius server del <id>                  : delete server
spadmin@Custservice177 ~ $
```

#### B) Configuration via web browser

**Management** -> **Authentication** page of the browser. Click “**Radius Setup**” button on left side of page



#### Adding/Removing a RADIUS Server

To add a RADIUS authentication server, or remove a server from the list:

1. Navigate to MANAGEMENT > OTHER: Authentication.
2. In the Actions panel on the left, click RADIUS Setup. The RADIUS Setup window will be displayed:



- **Host:** The hostname or IP address of the RADIUS server
  - **Port:** Defines the RADIUS Port to use. The default RADIUS Port is 1812, but this can be changed, as required.
  - **Secret Key:** The secret key which is shared by SecureSync and the RADIUS server (the key is used to generate an MD5 hash).



- **Timeout:** [seconds] Defines the Timeout that SecureSync will wait to communicate with the RADIUS server e.g., 10 seconds.

3. Click the Add Server button. A confirmation message The item has been added will be displayed if the server could be added, and the server will be added to the list, indicating its status (more info directly below)

**“Status” field**

The “Status” field in the row with the configured Radius server will report whether Radius is currently enabled and if the SecureSync can successfully reach that particular Radius server, as described below:

- **REACHABLE:** This RADIUS server can be reached.

indicates the **HTTP/HTTPS** checkbox at the top of the Radius Setup menu is currently selected (Radius is enabled) and the SecureSync can successfully reach the Radius Server. Note that “Reachable” does not show that the Secret Key has been entered correctly. It just shows it can see that the Radius server is on the network with the SecureSync. The Secret Key is verified by successfully logging in to the web browser using a Radius account.

**Status reports REACHABLE**

| Host        | Port | Timeout | Status                                         | Actions                          |
|-------------|------|---------|------------------------------------------------|----------------------------------|
| 10.2.100.92 | 1812 | 10      | <span style="color: green;">●</span> REACHABLE | <input type="button" value="x"/> |

- **DISABLED:** RADIUS service is disabled.

indicates the **HTTP/HTTPS** checkbox at the top of the Radius Setup menu isn’t currently selected. Press the “Radius Setup” button the left side of the page and select the **HTTPS/HTTPS** checkbox at the top of the “Radius Setup” menu. Then press Submit.

**HTTP/HTTPS checkbox not selected**



- **UNREACHABLE:** This RADIUS server cannot be reached.

indicates a Radius server that the SecureSync is not able to communicate with. The Host address may not be correct or the Radius server may not be on the same network as the SecureSync.

**Radius Server unreachable**



**Note:** See Radius troubleshooting on diagnosing this condition.

**Successful Radius login:**

**Auth log**

- **Successful Radius login** (with newer browser in 5.1.2 and above)

```
Jun  2 15:00:11 Spectracom apache2: pam_tally(login:account): pam_get_uid; no su
ch user
Jun  2 15:03:17 Spectracom apache2: pam_unix(login:account): could not identify
user (from getpwnam(oleg))
```

---

## Radius known issues/troubleshooting

- Refer to LDAP/Radius doc: [..\\..EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSyncLDAP and Radius](#)

### Known issues with Radius

#### 1) (applicable to version 5.8.6 only) CLI command response: **“You must be an administrator to invoke the model command”**

- Refer to Salesforce Case 217323 and JIRA Ticket SSS-748
- Software issue started in v5.8.6 and expected to be fixed in v5.8.7
- Affects both TACACS and RADIUS
- Issue described in the JIRA ticket

#### 2) (applicable to versions 5.8.4 and 5.8.5) kernel lockups/out of memory manager issues with Radius SSH

- Fixed in update version 5.8.6 (Oct 2019)
  - **Per the v5.8.5 Release Notes:** “Fixed an issue with TACACS+ and RADIUS causing kernel lockup, to improve responsiveness for SSH users.”

#### 3) After updating 5.0.2 to 5.1.4) Error message **“Error: The file you are trying to access does not exist on the server”** displayed when trying to login to the Classic interface

- Fix: Disable and then re-enable Radius (unselect and then re-select the “HTTP/HTTPS” checkbox)

#### 4) (version 5.1.2) Radius server add is broken

- Mantis case 2432: Radius server add is broken

Due to a file pointer issue in 5.1.2 (a pointer still pointing to a file for the classic interface -not moved over to the new web browser), Radius in the new web browser doesn't allow a user to be able to login. With the “Classic interface” web browser, if a user successfully authenticates with the Radius server, they are logged in, but only with user-rights (fields are greyed-out).

Radius works with classic interface but not with new interface.

#### 5) (v5.0.2 and below) Remote users can login but only have user rights (fields are greyed out)

- Mantis cases 2450 and 1555: Remote users can login but only have user rights (fields are greyed out)

Due to a permissions issue in v5.0.2, can't edit/configure the Radius configuration fields with 5.0.2 installed. If Radius fields were previously configured when the unit is updated to v5.0.2, this is no problem. But if it's cleaned after update to 5.0.2 or if trying to configure with 5.0.2 installed, this is an issue. Fix is to update to the next software release (or downgrade to previous, configure Radius as desired and then upgrade back to 5.0.2 again- but if it's cleaned, this has to be repeated).

#### 6) (all versions of at least 5.3.1 and below) Radius only supports HTTP/HTTPS connections

- This is a technical limitation of PAM

## 7) (v5.1.4 only) Radius in software version 5.1.4 (fixed in 5.1.5)

- If shipped w/5.1.4 already installed or if updated in the field and cleaned.

**Mantis case 2832: Per Ron Dries-** Not sure exactly why, but if the time server is clean updated from 5.1.3 to 5.1.4 (or shipped with 5.1.4 already installed) a user account needs to be created in the SecureSync in order to use this function. However, if it's updated from 5.1.3 to 5.1.4 without performing a clean, a user account does not need to be created. Suspect this will be fixed in the next software update.

**Email from Ron Dries, 30 May 2014** When I looked at the log I noticed that the PAM radius module was not being used, only the pam\_unix module. The new web UI uses a different PAM config file then the old web UI used. This means that if they still have the old config files from 5.0.2 then Radius could only be enabled in the old UI and not in the new UI. One way to test this would be to see if they can use radius to login to the old UI. I would suggest trying to disable and re-enable radius in the new UI which should enable the correct PAM config files.

By doing this however it might also require them to have to create the user on the box. Due to the issue we were talking about yesterday.

## 8) (versions 4.8.1 and below) "Not Supported" to be displayed in the LCD, even though the command did reset the password.

- With Archive Versions 4.8.1 and below installed, a minor bug causes "Not Supported" to be displayed in the LCD, even though the command did reset the password.

1) Is radius login to classic interface browser successful? If it is, the Radius Server settings are valid.

2) Get a full log bundle.

3) Review the User, Auth, Journal and System logs (especially both the Auth and User logs)

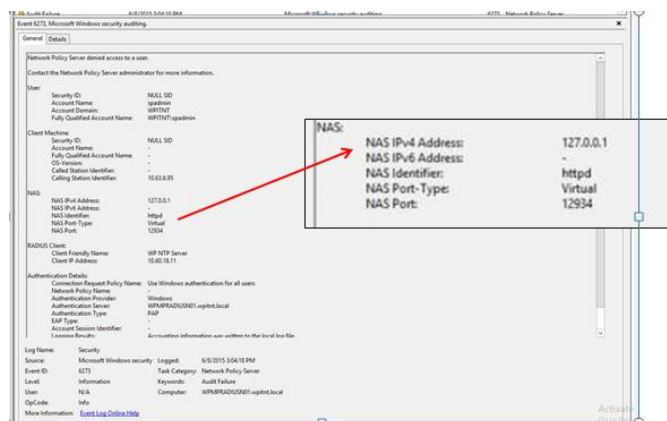
- Delete and re-enter the Radius server(s) using an intentionally wrong shared secret key and grab the logs. See if the System log contains the following entry **pam\_radius\_auth: packet from RADIUS server 10.82.122.16 fails verification: The shared secret is probably incorrect.** This entry indicates the SecureSync is communicating with the Radius server.
- Re-enter the Radius server using the correct Shared secret key and try logging in.

1) Make sure ports are open on firewalls between the SecureSync and the Radius server:

```
* radius      1812/tcp
* radius-acct 1813/tcp
* radius-dynauth 3799/tcp
```

2) **NAS address:** Are they possibly using the NAS address as a second layer of authentication (allowing only certain devices to be able to even contact the Radius server). Microsoft found our NAS address was being outputted in v5.2.0 and below as 127.0.0.1 which was blocking the SecureSync from even trying to authenticate (instead of it being the IP address of the SecureSync). This is expected to be addressed in 5.2.1. Refer to Mantis case 3017 and Salesforce case

**Example screenshot showing SecureSync reporting its NAS address as its loop back address instead:**



## Details about the NAS address

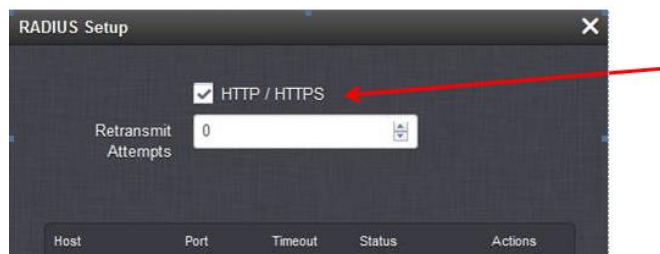
- Refer to Salesforce cases 17439 and 18482.
- In versions 5.2.0 and below, the NAS address is always the loopback address of 127.0.0.1
- Starting in version 5.2.1:
  - If the SecureSync can't find a DNS server, its NAS address will remain its loopback address of "127.0.0.1"
  - If the SecureSync finds a DNS server, the SecureSync will then change its NAS address to the IP address it receives from the DNS server (which is the IP address that has been mapped to its hostname within the DNS server).

If the NAS address is the wrong address for the SecureSync and as long as it's not still 127.0.0.1 (indicating an issue with the SecureSync finding the DNS server) the DNS server needs to be checked to ensure the SecureSync's hostname has been mapped to the correct IP address. The SecureSync just reports the NAS as the address it gets from the DNS.

**Note:** Valid LDAP logins do not result in any User or Auth log entries.

## Notes about updating to 5.1.4 from previous revs

- A) When updating from 5.1.3 to 5.1.4- if it's clean updated from 5.1.3 to 5.1.4, a user account needs to be created in the SecureSync in order to use this function. However, if its updated from 5.1.3 to 5.1.4 without performing a clean, a user account does not need to be created. Suspect this will be fixed in the next software update.
- B) When updating from v5.0.2 and below (classic interface) to the new browser (v5.1.2 and above), Radius configs brought forward during the update are still setup for the classic interface. Login to the new browser will fail, but login to the classic interface should work.
- C) To verify Radius is configured correctly should initially be able to login to the classic interface using Radius.
- D) Once radius has been verified with classic interface, disable and then re-enable Radius (Management -> Authentication page, click on the Radius Setup button on the left side of the page). Unselect the "HTTP/HTTPS" checkbox and press Submit. Then select this same checkbox and press Submit again.



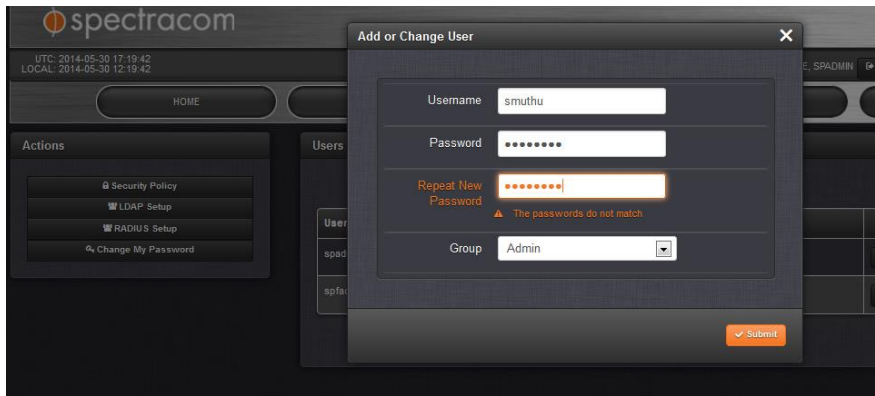
Radius login should now be setup to work with the new browser, instead of the classic interface. Try logging in with the Radius account/password.

If can't login to the browser using the account only in the Radius server, a user account will need to be temporarily created in the SecureSync (until a software update addresses this requirement). If an account needs to be created -The username has to be the same as the radius username, but the account password does not need to be the same as the Radius password for it to work.

In some cases, after updating to version 5.1.4 from an earlier version of software, a local user account needs to be created in the Time server in order to use Radius login with this version installed. A future software update will alleviate the need to have a local account in the SecureSync,

When creating a user account, the username has to be the same as the Radius account name. However, the required password to create the account does not need to be the same as the Radius password.

If you haven't already created a user account with the name of "smuthu" for example, go to the **Management -> Authentication** page of the new browser. Then click on the "+" sign in the upper-right corner (just above the "search" field). Enter the desired Radius Username and any desired password (doesn't have to be the same as the Radius account password). Then select the "Admin" Group and press Submit.



After creating the user account, try logging in again using the same Radius account name and the Radius password.

## C) General Radius troubleshooting

### Radius troubleshooting tips/summary

#### CLI command to list all users

**Per Ron Dries (21 April 2020)** For a command line way to list users, including LDAP users, issue the following command:  
**getent passwd**<enter>

1. Check software version installed:
  - If customer is using NAS for second level authentication, software version in the time server needs to be **at least version 5.2.1** due to issue with NAS address reported by the SecureSync in v5.2.0 and below.
2. refer to Radius/LDAP tech note
3. get full logs/configs bundles (review especially the Auth, Journal and User logs. More info further below)
4. Review Radius config files (more info further below)
5. Try logging into the classic interface browser (while still available in the software) using credentials only in the Radius server.
6. Try momentarily disabling and re-enabling Radius. Then logout of the browser and try logging in again using credentials only in the Radius server.
7. get a wireshark/tcpdump capture (more info further below)
  - Use **tcpdump** (versions 5.2.1 and above) to see the request and accept messages (see info further above) Make sure the packets are on the correct Ethernet interface to be able to reach the Radius server.
8. Is HTTP/HTTPS checkbox at the top of the **Management -> Radius Setup** config page selected?
9. Is the Radius Setup page showing the Radius server is "reachable" (responding to ping).
  - second level authentication, software version needs to be at **version 5.1.5** due to issues in earlier versions
10. Any firewalls in between with TCP ports 1812, 1813 or 3799 closed?

#### Draft email for initial troubleshooting

In order for us to be able to better assist you with getting Radius login to the web browser working, please:

Send us a screenshot of the Tools -> Upgrade/Backup page of the web browser (if it's still accessible) showing that the SecureSync has been updated to version 5.2.1 (per Dave's earlier recommendation). If it's not accessible, please send a copy of the response to the following CLI command: `version` <enter> to show the current version of software.

Send us a screenshot of the Management -> Authentication page, Radius Setup button in the browser (if it's still accessible). A full copy of all the unit's logs for our review (via the CLI interface command and FTP/SCP, if you aren't able to access the

browser any longer using the spadmin account)

## Logs

- get logs/configs bundles (review especially the Auth and Uuser logs)
  - **View Auth log Via CLI:** Spectracom/home/spectracom/log and then type **cat auth.log**

### To obtain all of the logs via the web browser (if it's still accessible):

All of the SecureSync's logs (including those shown in the browser and also those in the background) can be easily bundled into one file and then exported from the SecureSync to send as an attachment.

Instead of copy/pasting all of the log entries into a Word document, starting in Archive software update version 5.1.2, the logs can be easily saved to single bundled file and exported into a networked PC. Earlier versions of software allowed the bundle to be created, but then the file still needed to be transferred out using an FTP/SCP connection. Now, a button in the web browser alleviates the need to create an FTP session to transfer this file out to a PC.

The log bundling and export to a PC is controlled in the "**Management**" -> "**Log Configuration**" page of the SecureSync's web browser. On the left-side of the browser, click on the "**Save and download all logs**" button. You can then select where to save the log bundle to. The default file name is "seuresync.log".

### To obtain all the logs via the CLI interface if the browser is not accessible

- 1) Login the CLI interface via telnet or ssh.
- 2) Type **savelog** SecureSync <enter>
- 3) Login to the CLI interface using an FTP or SFP utility and navigate to the following directory:  
**/Home/Spectracom/Xfer/Log**
- 4) Transfer out this log file and send it to us as an attachment. Note that you may need to zip the file due to its size.

---

## Example user.log log entries (connection to radius server issues)

### 1) No Radius servers found

apache2: pam\_radius\_auth: No RADIUS server found in configuration file /etc/raddb/server

**Cause:** No Radius servers have been configured. Need at least one server to be added. Verify configuration of the **Management -> Authentication** page of the browser. Click "**Radius Setup**" on the left side of the page.

### 2) Servers failed to respond

apache2: pam\_radius\_auth: RADIUS server 10.2.100.92 failed to respond

apache2: pam\_radius\_auth: All RADIUS servers failed to respond

**Cause:** Invalid Radius server address(es) or network issue exists. Verify configuration of the **Management -> Authentication** page of the browser. Click "**Radius Setup**" on the left side of the page.

### 3) Shared secret key is incorrect

apache2: pam\_radius\_auth: packet from RADIUS server 10.2.100.92 fails verification: The shared secret is probably incorrect.

apache2: pam\_radius\_auth: All RADIUS servers failed to respond.

**Cause:** Valid server, valid port, **but wrong Secret Key** entered in Radius configuration. Verify configuration of the **Management -> Authentication** page of the browser. Click "**Radius Setup**" on the left side of the page.

---

## Example auth.log log entries (authentication with radius server issues)

**Note:** to see the latest entry of the user log: **tail -f log/auth.log** (or change to the log directory and then type):  
**tail -f auth.log**

### Cause: invalid Radius server address

```
Sep 12 21:54:19 CustService-176 unix_chkpwd[6256]: password check failed for user (oleg)
Sep 12 21:54:19 CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001
tty= ruser= rhost=10.2.100.124 user=oleg
Sep 12 21:54:19 CustService-176 apache2: pam_tally(httpd:auth): conversation failed
Sep 12 21:54:19 CustService-176 apache2: pam_tally(httpd:auth): user oleg (1052) tally 15, deny 5
```

### Cause: wrong username and ambiguous password

```
Sep 12 21:47:19 CustService-176 apache2: pam_securetty(httpd:auth): cannot determine user's tty
Sep 12 21:47:19 CustService-176 apache2: pam_unix(httpd:auth): check pass; user unknown

Sep 12 21:47:19 CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001
tty= ruser= rhost=10.2.100.124
Sep 12 21:47:19 CustService-176 apache2: pam_tally(httpd:auth): pam_get_uid; no such user
```

### Cause: right username but wrong password

```
Sep 12 21:44:09 CustService-176 unix_chkpwd[30024]: password check failed for user (oleg)
CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser=
rhost=10.2.100.124 user=oleg
CustService-176 apache2: pam_tally(httpd:auth): conversation failed
CustService-176 apache2: pam_tally(httpd:auth): user oleg (1052) tally 11, deny 5
```

### Cause: right server IP address, but wrong port number configured

```
Sep 12 21:59:00 CustService-176 unix_chkpwd[25159]: password check failed for user (oleg)
Sep 12 21:59:00 CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001
tty= ruser= rhost=10.2.100.124 user=oleg
```

## Questions that may help determine the cause of this issue:

- 1) Just to confirm, all three units have the same Archive version 4.8.4 software installed (as indicated on the Tools/Versions page)?
- 2) Are all three Model 9483s, at least temporarily, placed on the same subnet? (for instance, are you putting each one individually on the network, using the same IP address for each NTP server, or plugging all three into the same subnet at the same time by using different IP addresses)? Or, instead, are they located on different subnets or different networks altogether?
- 3) If they are installed in different subnets or isolated networks, have you tried swapping the one unit with either of the other two to see if the issue follow
- 4) Are there any firewalls between the Radius server and the NTP servers?
- 5) Just to confirm, all the Radius configurations in the Network/ Radius Setup page of the browser (in both the "General Settings" and "Server Configuration" tabs) are exactly the same in all three time servers?
- 6) Is the table located in the Network/General Setup page of the browser, "Access" tab, empty in all of the units?
- 7) Do the three units you received have this available Option Card installed? Or, is there only one network port on the back of each of the three units?
- 8) If this Option Card is installed, is the network connected to the base Ethernet port on the main chassis, or one of the three ports on the installed Option Card installed on the Option Bay?
- 9) With this Model 9483 connected to the network and Radius not working, have you tried to ping, telnet, FTP or SSH in (which will all indicate whether the specific port is operational). If not, I recommend first trying to ping and then telnet into the NetClock's address, via the command prompt window, or ssh or ftp in using an ssh/ftp program (such as puttySSH or CoreFTP).

**Note:** If you can't ping, telnet, ssh or FTP connect to the NTP sever, this indicates a network port issue exists.

10) If this Option Card is installed, have you tried connecting to one of the other three network ports (with that other port configured with a similar IP address)? If not, I recommend trying this to ensure there isn't a problem with that one particular port.

11) Are you using dynamic/DHCP IP addresses or static IP addresses?

To reset all of the configs and logs back to factory default values, perform a "clean" CLI command. A "clean" command can be performed by connecting a PC running HyperTerminal (or other terminal emulator software) to the front panel SERIAL port with a straight-thru DB8F to DB9F serial cable. The settings for HyperTerminal are 9600, N, 8 1. ).

Once connected, type: **clean** <enter>. Note that this same command can also be sent with a telnet or an SSH connection (as long as these services are still enabled in the web browser). Either telnet or ssh into the NTP server and then type: clean <enter>. After issuing this command via RS-232, telnet or SSH, the logs and configurations will be reset and the web browser should be accessible again. Then just configure the SecureSync as desired. **Note:** An automatic reboot is performed when performing a Clean command

## Radius not working on a unit

I verified with our engineering team that there are no hardware issues that can cause an issue specific to only Radius connection (as I suspected). Any potential hardware issues with the Model 9483 itself that affect Radius would have to also affect network connectivity in general on that port. So, along these lines, we want to make sure whichever network port on the Model 9483 that the network is connected to is able to successfully communicate with the network. All Model 9483s have an available base Ethernet port ("eth0"). However, the Model 9483 also has an available Option Card (Called the "Gigabit Option Card", Model 1204-06) that can be installed in a rear panel Option Bay to add three additional network ports (eth1, eth2 and eth3) to the Model 9483.

FYI- Software version 4.8.0 added standard Linux "out-bound" network tools to the Model 9483's Command Line Interface (CLI). These network tools can be helpful with troubleshooting network-related issues.

If you connect to the Model 9483 via the front panel RS-232 SERIAL port, or over network via telnet or ssh, try pinging the IP address of the Radius server. With a good network connection between the time server and the Radius server, the Radius server should continue to respond to pings, until you press CTRL/C.

### \*\*\*Radius ports (UDP)

#### UDP Port 1812 (Radius authentication messages)

- When Radius is enabled, the SecureSync is a Radius client
- UDP Port 1812 is the typical port to use for Radius
- When Radius is enabled, the SecureSync doesn't listen on port 1812. The SecureSync only transmits (and only transmits when someone is actively logging into the web browser)
- Because the SecureSync doesn't listen on UDP port 1812, it won't show up in a netstat response or other port sniffer program.
- To see UDP port 1812 listening, run **netstat** on the radius server itself, as the radius server listens for Radius clients on port 1812

#### A) Radius server reporting "unreachable"

1. Is ping disabled in Radius server
2. in CLI perform the following command: **tracert -p xxx yyy.yyy.yyy** (where xxx is radius port, such as 1812 and where yyy is the address for the Radius server. Make sure response indicates the radius server was reachable.



## B) Cant enable Radius Service

1. make sure at least one Radius server has been listed (added via the Add Server button)
2. Refer to Salesforce cases such as 173674 (v5.8.0 installed)

## C) Browser displays “Password expires today” (versions 5.1.2 to 5.1.7)

- **Note:** Software update 5.2.0 removes the “Password expires today” message. No longer displayed.

### Email from Ron Dries (6 Oct 2014 regarding Password Expires today” message)

The password expired message appears because the RADIUS user’s information is not located on the box. When the UI does a check for the age of the users password that information cannot be found, and the UI then thinks that the users password has expired.

I’m not sure if this was intended or not, however I think the UI should not report the password is expired because we don’t have control over remote user accounts. I’ll take a look at it and see what modifications can be made to not show this message if the user cannot be found on the SecureSync

## Tcpdump capture of radius traffic

**Note: omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE**

- Version 5.2.1 added tcpdump to the SecureSync.
- To see the messages being sent to the Radius server, login to the CLI via telnet or ssh. Then type: **sudo tcpdump udp port 1812**. Then with Radius configure/enabled, login to the web browser. (Note this particular command looks on eth0 only. The port will need to be specified in this command if the Radius server is on a different Ethernet interface than eth0):

- A) Example below is from a **successful Remote login to the “oleg” account** (not stored in the SecureSync). Port 1812

```
tcpdump: syntax error
spadmin@custservice177 ~/log $ sudo tcpdump udp port 1812
error : ret -1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:22:11.576348 IP 10.2.100.177.25076 > 10.2.100.31.radius: RADIUS, Access Request (1), id: 0x39 length: 2
12:22:11.583317 IP 10.2.100.31.radius > 10.2.100.177.25076: RADIUS, Access Accept (2), id: 0x39 length: 2
```

- B) Example below is from a **failed radius login attempt** (invalid configurations for the radius server- wrong address wrong key. Etc) Notice there is AN Access Request sent from the SecureSync but no Access Accept sent back from the Radius server. Port 1812.

```
spadmin@custservice177 ~/log $ sudo tcpdump udp port 1812
error : ret -1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:45:14.566692 IP 10.2.100.177.codasrv > 10.2.1.2.radius: RADIUS, Access Request (1), id: 0x17 length: 90
```

## \*\*\*\*\*Radius configuration file

- Customers can view the Radius login config file with the spadmin account
  - `/etc/pam.d` and then type: **cat login**
  - Radius is controlled in `/etc pam.d`
- **Path to Radius configuration:** `cd /etc/pam.d/radius` Then type either: **cat httpd** or **cat login** (example from v5.3.0 below):

```
spfactory@Spectracom /etc/pam.d $ cat httpd
# Radius Version
auth sufficient pam_radius_auth.so retry=0
account sufficient pam_radius_auth.so
session sufficient pam_radius_auth.so
auth required pam_securetty.so
auth required pam_unix.so try_first_pass
auth required pam_tally.so deny=5 unlock_time=60 per_user
account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account required pam_deny.so
session required pam_unix.so
session required pam_limits.so
spfactory@Spectracom /etc/pam.d $
```

- Per Ron Dries, the radius settings are stored in `/etc/raddb` (the file is named "server" so type: **cat server**)

Example Radius config file ("server") in `/etc/raddb/server` (can be viewed in spadmin account)

```
spadmin@Spectracom /etc/raddb $ cat server
#retry 0
10.2.100.31:1812 7cqptkHwjuGnvrL 10
spadmin@Spectracom /etc/raddb $
```

File from our NetClock with Radius working correctly:

```
spadmin@Spectracom/etc/pam.d
Password:
Spectracom NetClock 9483 Version 5.1.4
spadmin@Spectracom ~ $ cd /etc/pam.d
spadmin@Spectracom /etc/pam.d $ cat login
# Radius Version
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth sufficient pam_radius_auth.so retry=0
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
#account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account sufficient pam_radius_auth.so
account required pam_deny.so
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session sufficient pam_radius_auth.so
session required pam_unix.so
password required pam_unix.so shadow md5
spadmin@Spectracom /etc/pam.d $
```

**Viewing all accounts via the CLI interface:** Spectracom/etc and type: **getent shadow**. Scroll down to the bottom of the response.

**Note:** Refer to “Shadow” in the “all products” section at the beginning of this document for deciphering this response.

```
spfactory@Spectracom/etc $ getent shadow
halt:*:9797:0:0:0:
operator:*:9797:0:0:0:0:
shutdown:*:9797:0:0:0:0:
sync:*:9797:0:0:0:0:
bin:*:9797:0:0:0:0:
daemon:*:9797:0:0:0:0:
adm:*:9797:0:0:0:0:
lp:*:9797:0:0:0:0:
news:*:9797:0:0:0:0:
uucp:*:9797:0:0:0:0:
nobody:*:9797:0:0:0:0:
man!:15818:0:0:0:0:
sshd!:15818:0:0:0:0:
cron!:15885:0:0:0:0:
dhcp!:15885:0:0:0:0:
ftp!:15885:0:0:0:0:
ntp!:15885:0:0:0:0:
stunnel!:15885:0:0:0:0:
ldap!:15885:0:0:0:0:
apache!:15885:0:0:0:0:
nullmail!:15885:0:0:0:0:
feron!:15885:0:0:0:0:
mysql!:15885:0:0:0:0:
spui!:16176:0:99999:7:0:
spadmin:$1$a0P9NVVT$8V0U8EP7awhQs63mg9vRT.:16176:0:99999:7:0:
root:$1$z0.7Xhnt$yjdYK51.IVAVVLI.hIbpK.:16176:0:0:0:0:
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:16176:0:99999:7:0:
oleg:$1$gwwumFVb$AOjilsgsfZH4RWAatFiRO/:16189:0:99999:7:0:
spfactory@Spectracom/etc $
```

### \*\*\*NAS (Network Access Server)

#### NAS-IP address

- Update Version 5.2.1 improved how Radius detects and fills in NAS-IP address in its packets.
- This change adversely affected another customer (Logix)
- Version 5.3.0 is reverting the changes in version 5.2.1 in a way that will be better for all customers without breaking it for Microsoft.

**From the v5.3.0 Release Notes:** Fixed an error causing Radius authentication to fail because the NAS address is being output as 127.0.0.1.

### \*\*\*Permissions assigned to Radius accounts

#### Software versions 5.6.0 and above

- Update version 5.6.0 added ability for Radius (and tacacs) to remote authenticate both the browser login and now also CLI interface, alleviating need to have an account stored on the box for CLI

#### Software versions 5.5.1 and below

- **Note:** Software **version 5.6.0** (Apr 17) added login user authentication support for protocols other than HTTP/HTTPS (web browser). Now supports CLI interface as well (such as ssh, telnet and FTP/SCP)
- All users that login via a Radius account are assigned RW (Read/Write) permissions.
- It's not currently possible to have a Radius account assign RO (Read Only) permissions
- Email from Morgan to Microsoft: “Our radius implementation only checks authentication, so there is no way to give a user READ-ONLY access”
- To assign Read Only (RO) permissions, need to create a custom user account in the SecureSync and that user needs to be assigned to the users group.

### Admin/User rights for Radius users

- All users who login to the SecureSync through Radius are automatically assigned Admin rights.
- Radius accounts can't be assigned user rights, unless either Radius authentication is combined with LDAP Authentication as well, or a local user account is created in the SecureSync.
- RADIUS only provides authentication. You provide it a username and a password, and it provides back whether that username and password is authenticated. It doesn't provide any permissions or other authorization information. The only alternatives to allow accounts to have user rights (instead of admin rights) are to either:
  1. Combine RADIUS with another system that provides authorization (such as LDAP),
  2. Or to make local user accounts matching those that are being authenticated.
- If there is a local account with the same username, it will be authenticated using RADIUS, and use the permissions from the local account.

---

### Ability to disable LDAP/Radius via the front panel to regain access to locked-out unit.

- **resetpw** (in the front panel "cmd" menu) disables LDAP/Radius (versions 5.3.0 and above)

**Note:** Starting in version 5.2.1 (~~Apr 2015~~) **resetpw also sets LDAP and Radius to "Disabled"** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026 Update- this change was **inadvertently left out of the v5.2.1 release. It will need to be added in version 5.3.0**

When resetpw is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled as desired, after performing a resetpw command.

Q Help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?

**A Keith's response (23 May 17)** Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of 'admin123'.

Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn't change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.

## LDAP

### Our LDAP Server

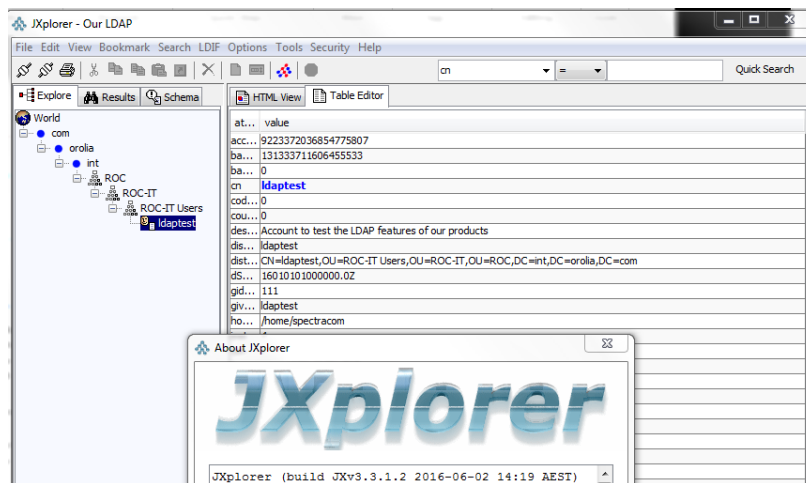
- Set up and maintained by IT team
- (for old software versions such as 5.4.1 and below) Refer to <S:\Projects\Lafayette\301 Verification Test Results> for the settings (these are for very early software versions)

### PVP (Product Verification) for each Software Release

**Note:** For example engineering software release testing of Radius, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 [https://app.bom.com/changes/detail-summary?change\\_id=2389346979](https://app.bom.com/changes/detail-summary?change_id=2389346979)) to find the PVP Test validation in the list of "ITEMS"

### Active Directory/schema viewer to see the directory structure of the IT's AD server

- Example of a freeware/opensource viewer: JXplorer



For testing, use our time server **10.2.100.176** (**Note:** On 6 Feb 2017, I configured and successfully used LDAP on on unit at 10.2.100.215. Apparently, our LDAP server isn't configured to only work with 10.2.100.176).

**Management -> Authentication** page and click **LDAP**

Refer to:

- **SecureSync Tech Note:** <EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\LDAP and Radius>
- **Model 9400 Tech Note:** <EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\LDAP and Radius>

**LDAP/RADIUS RFCs (in this document):** [\\*\\*Port assignments and RFCs for all products](Port assignments and RFCs for all products)

**OpenLDAP:** <http://www.openldap.org/>

**Shortcut to SecureSync LDAP/Radius design info:** <S:\Projects\Lafayette>

### Order of precedence for both Radius and LDAP when logging in (Per Ron)

- Radius authentication is attempted
- LDAP authentication is attempted.
- Local login (accounts in the NTP server).

As indicated: (internal use only) Spectracom/etc/pam.d/radius and type: **cat login**

```
spadmin@ntp1-pwy-2/etc/pam.d
spadmin@ntp1-pwy-2 ~ $
spadmin@ntp1-pwy-2 ~ $ cd /etc/pam.d
spadmin@ntp1-pwy-2 /etc/pam.d $ cat login
# Radius Version
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth [success=ok perm_denied=1 default=ignore] pam_spectracom.so
auth sufficient pam_radius_auth.so retry=0
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
#account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account sufficient pam_radius_auth.so
account required pam_deny.so
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session sufficient pam_radius_auth.so
session required pam_unix.so
password required pam_unix.so shadow md5
spadmin@ntp1-pwy-2 /etc/pam.d $
```

## Our LDAP configuration

### Tabs

#### Settings Tab

**Check “Enabled”**

**Server type** = Active Directory

**Search Base DN** dc=int,dc=orolia,dc=com

**Bind DN** (“Distinguished name”)

CN=ldaptest,OU=ROC-IT Users,OU=ROC-IT,OU=ROC,DC=int,DC=orolia,DC=com

**Bind Password:** Password12 (note: may not accept certain special characters)

**NSS Password** OU=ROC-IT,OU=ROC,?sub

(Note: “NSS allows administrators to specify a list of sources where authentication files, host names and other information will be stored and searched for”)

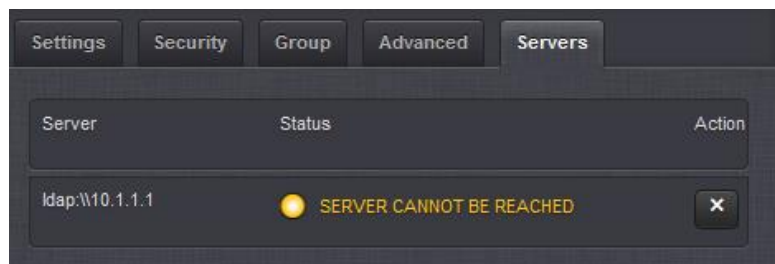
#### Servers Tab

**Add an additional server:** **ldap://rocdc01.int.orolia.com**

**Note:** to use its IP address instead: **ldap://10.1.1.26/**

**Note:** After entering the LDAP server address, if the “Servers” tab reports “Invalid Configuration, please...” (instead of “LDAP Configuration valid”) verify the “DNS primary” address in Eth0 is set to “10.1.1.20. Missing or incorrect DNS server address will cause this to occur.

**Note:** After entering the LDAP server address, if the “Servers” tab reports “server cannot be reached” (instead of “LDAP Configuration valid”)



### Verify:

- 1) Whether using the LDAP server's IP addresss or hostname, the Server line must begi with **ldap://** (and **not "ldap:\\"**)
  - Example above shows the wack/wack going in the wrong direction (instead of \\, it should be //)
- 2) (if using a hostname instead of IP address) DNS is configured correctly and working (try temporarily using its IP address to see if it then connects. If it does, there is a DNS-related issue.
- 3) make sure all the LDAP settings (in the Settings tab) are correct. these do affect the adding of a server.

### Group Tab

**Enable group filter:** not selected  
All three fields empty

### Advanced Tab

**Search Filter:** objectclass=user  
**Login Attribute:** sAMAccountName  
**Verify Certificate (checkpeer):** Not selected

### Close browser and Login with:

**Username:** ldaptest  
**Password:** Password12

**Email from Steve Hailstone:** I also put a certificate in I:\engineering\ldap cert. There are different file types that the cert can be so once again may need to experiment.

---

Viewing all accounts via the CLI interface: Spectracom/etc and type: **getent shadow** <enter> Scroll down to the bottom of the response.

**Note:** Refer to “Shadow” in the “all products” section at the beginning of this document for deciphering this response.

```
spfactory@Spectracom/etc
spfactory@Spectracom /etc $ getent shadow
halt:*:9797:0:0:0:
operator:*:9797:0:0:0:
shutdown:*:9797:0:0:0:
sync:*:9797:0:0:0:
bin:*:9797:0:0:0:
daemon:*:9797:0:0:0:
adm:*:9797:0:0:0:
lp:*:9797:0:0:0:
news:*:9797:0:0:0:
uucp:*:9797:0:0:0:
nobody:*:9797:0:0:0:
man!:15818:0:0:0:
sshd!:15818:0:0:0:
cron!:15885:0:0:0:
dhcp!:15885:0:0:0:
ftp!:15885:0:0:0:
ntp!:15885:0:0:0:
stunnel!:15885:0:0:0:
ldap!:15885:0:0:0:
apache!:15885:0:0:0:
nullmail!:15885:0:0:0:
fcron!:15885:0:0:0:
mysql!:15885:0:0:0:
spui!:16176:0:99999:7:0:
spadmin:$1$a0P9NVVT$8VOU8EP7awhQs63mg9vRT.:16176:0:99999:7:0:
root:$1$z0.7Xhnt$yjdyK51.IVAVVLI.hIbpK.:16176:0:0:0:
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:16176:0:99999:7:0:
oLeg:$1$gwwumFVb$AojilsgsEZH4RWAatFiR0/:16189:0:99999:7:0:
spfactory@Spectracom /etc $
```

To view the LDAP config file after editing, type **cat /etc/ldap.conf** <enter> (ctrl x to escape)

```
spadmin@Custservice177 ~ $ cd /etc
spadmin@Custservice177 /etc $ cat ldap.conf
version 3
scope sub
timelimit 120
bind_timelimit 120
base dc=int,dc=orolia,dc=com
binddn CN=ldaptest,OU=ROC-IT Users,OU=ROC-IT,OU=ROC,DC=int,DC=orolia,DC=com
bindpw Password12
tls_checkpeer no
# ad
pam_filter objectclass=user
pam_login_attribute sAMAccountName
nss_base_passwd OU=ROC-IT,OU=ROC,?sub
nss_base_shadow OU=ROC-IT,OU=ROC,?sub
nss_map_objectclass posixAccount User
nss_map_objectclass shadowAccount User
nss_map_attribute uid sAMAccountName
nss_map_attribute cn sAMAccountName
nss_map_attribute uniqueMember member
nss_override_attribute_value unixHomeDirectory /home/spectracom
nss_override_attribute_value LoginShell /bin/bash
bind_policy soft
spadmin@Custservice177 /etc $
```

## LDAP configuration:

- Refer to sites such as: [https://technet.microsoft.com/en-us/library/cc755809\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc755809(v=ws.10).aspx)

What connections are controlled by LDAP (when LDAP is enabled)?

- 1) Web browser
- 2) Telnet/SSH/FTP/SCP
- 3) Front panel serial port

**Note:** all of these are automatically controlled when LDAP is enabled. There is no individual enabling for each.



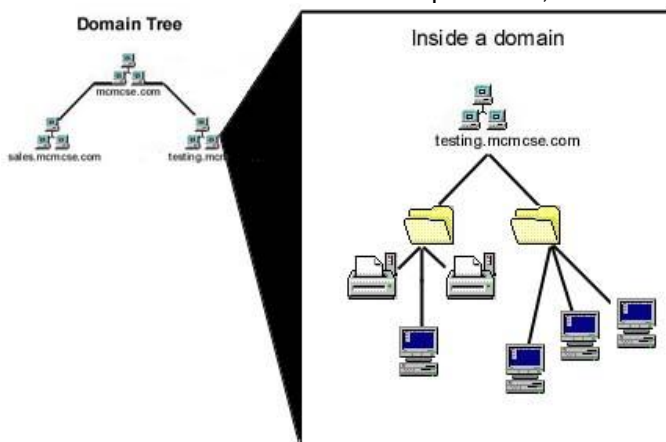
From: <http://www.mcmcse.com/microsoft/guides/ad.shtml>

### Directory Components:

what happens inside a domain? To get started, the first concept that you will need to understand what the directory is made of. A common analogy for a directory is a phonebook. Both contain listings of various objects and [information](#) and properties about them. Within the directory are several other terms that you must know to gain even an entry level understanding as to how it all works.

- **Objects** - Objects in the database can include printers, users, servers, clients, shares, services, etc. and are the most basic component of the directory.
  - **Attributes** - An attribute describes an object. For example, passwords and names are attributes of user objects. Different objects will have a different set of attributes that define them, however, different objects may also share attributes. For example, a printer and Windows Vista computer may both have an IP address as an attribute.
  - **Schema** - A schema defines the list of attributes that describe a given type of object. For example, let's say that all printer objects are defined by name, PDL type and speed attributes. This list of attributes comprises the schema for the object class "printers". The schema is customizable, meaning that the attributes that define an object class can be modified.
  - **Containers** - A container is very similar to the folder concept in Windows. A folder contains files and other folders. In Active Directory, a container holds objects and other containers. Containers have attributes just like objects even though they do not represent a real entity like an object. The 3 types of containers are Domains, Sites and Organizational Units and are explained in more detail below.
- *Domains* - We have already discussed this concept in the preceding paragraphs.
- *Sites* - A site is a location. Specifically, sites are used to distinguish between local and remote locations. For example, company XYZ has its headquarters in San Fransisco, a branch office in Denver and an office that uses DUN to connect to the main network from Portland. These are 3 different sites.
- *Organizational Units (OU)* - Organizational units are containers into which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains. The fact that organizational units can contain other OUs, a hierarchy of containers can be created to model your organization's structure and hierarchy within a domain. Organizational units should be used to help minimize the number of domains required for a network.

Now that we know what these concepts mean, let's take a visual look at what is going on inside a domain.



The folder symbols represent Organizational Unit (OU) containers and within each of these we find objects such as printers, [servers](#), computers, users, etc. Instead of objects directly located inside these OUs, there could be more OU containers.

### Object Names:

Active Directory uses the Lightweight Directory Access Protocol (LDAP) to supply the naming convention for objects. The 2 basic concepts that you need to know are distinguished names and common names. Distinguished names are the complete "path" through the hierarchical tree structure to a specific object. This is similar to specifying the complete path to a [file](#) from a DOS prompt. This "path" points to the location of an object in the

hierarchy. Let's take a look in more detail.

## Distinguished Name (DN)

➤ The following are the components that make up a distinguished name:

- **OU - Organizational Unit.** This attribute is used to divide a namespace based on organizational structure as previously discussed. An OU usually is associated with an Active Directory container or folder.
- **DC - Domain Component.** Domain components. A distinguished name that uses DC attributes will have one DC for every domain level below root. Another way of thinking of this would be that there would be a DC attribute for every item separated by a dot in the domain name.
- **CN - Common Name.** This attribute represents the object itself within the directory service.

**Note:** Indented info below is from [https://technet.microsoft.com/en-us/library/cc755809\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc755809(v=ws.10).aspx)

### Distinguished Name

Every object in Active Directory has a distinguished name (also known as DN). A distinguished name uniquely identifies an object by using the name of the object, plus the names of the container objects and domains that contain the object. Therefore, **the distinguished name identifies the object as well as its location in a tree.** The distinguished name is unambiguous (that is, it identifies one object only) and unique (that is, no other object in the directory has this name). It contains enough information for an LDAP client to retrieve the object's information from the directory.

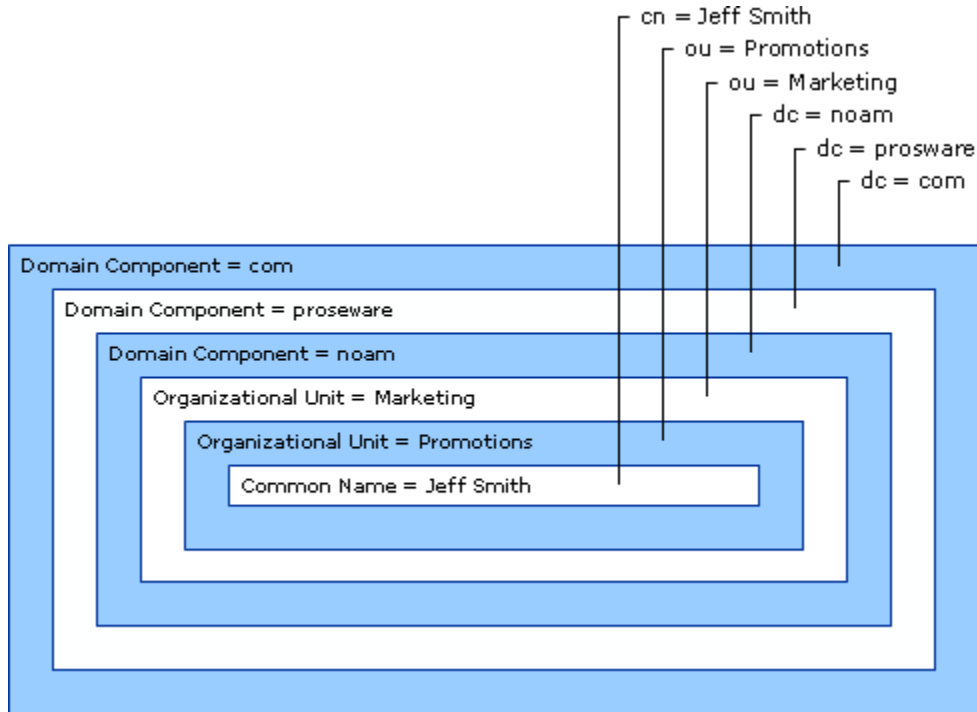
For example, a user named Jeff Smith works in the marketing department of a company as a promotions coordinator. His user account is created in an OU that stores the accounts for marketing department employees who are engaged in promotion activities. The root domain of the company is proseware.com, and the local domain is noam.proseware.com. The distinguished name for this user object is:  
cn=Jeff Smith,ou=promotions,ou=marketing,dc=noam,dc=proseware,dc=com

### Relative Distinguished Name

The relative distinguished name (also known as the RDN) of an object is the part of the distinguished name that is an attribute of the object itself — the part of the object name that identifies this object as unique within a container. For the example in the previous paragraph, the relative distinguished name of the user object:  
cn=Jeff Smith,ou=promotions,ou=marketing,dc=noam,dc=proseware,dc=com  
is cn=Jeff Smith.

The following figure illustrates the relative distinguished names that make up the distinguished name of the user object Jeff Smith.

## Relative Distinguished Names That Make Up a Distinguished Name



The maximum length that is allowed for a relative distinguished name is 255 characters, but attributes have specific limits that are imposed by the directory schema. For example, in the case of the common name (cn), which is the attribute type that is often used for naming the relative distinguished name, the maximum number of characters that is allowed is 64.

Active Directory relative distinguished names are unique within a container; that is, Active Directory does not permit two objects with the same relative distinguished name under the same parent container. However, two objects can have identical relative distinguished names but still be unique in the directory because, within their respective parent containers, their distinguished names are not the same. For example, the object `cn=Jeff Smith,cn=users,dc=noam,dc=proseware,dc=com` is recognized by LDAP as being different from `cn=Jeff Smith,ou=marketing,dc=noam,dc=proseware,dc=com`.

The relative distinguished name for each object is stored in the Active Directory database. Each object in the directory contains a reference to the parent of the object. An LDAP operation can construct the entire distinguished name by following these references to the root.

### Default Active Directory Naming Attributes

| Object Class       | Naming Attribute Display Name | Naming Attribute LDAP Name |
|--------------------|-------------------------------|----------------------------|
| user               | Common-Name                   | cn                         |
| organizationalUnit | Organizational-Unit-Name      | ou                         |
| domain             | Domain-Component              | dc                         |

Each portion of the distinguished name is expressed as `attribute_type=value`. The attribute type that is used to describe the object's relative distinguished name (in the Jeff Smith example, cn) is called the naming attribute. In Active Directory, instances of classes have a default mandatory naming attribute that is defined in the schema. For example, part of the definition of the class user is the attribute cn (Common-Name) as the naming attribute. Therefore, the relative distinguished name for user Jeff Smith is expressed as `cn=Jeff Smith`.

Classes that do not define a naming attribute inherit the naming attribute from their parent class. If you create a new class in the Active Directory schema (that is, if you create a new classSchemaobject), you can use the

optional rDNAttID attribute to specify the naming attribute for the class.  
The following table shows the naming attributes that are used in Active Directory.

**Here is an example of a distinguished name:**

CN=Jason Sprague,CN=Users,DC=mcmcse,DC=COM

Now let's say that I was a member of the [sales.mcmcse.com](http://sales.mcmcse.com) domain. My new DN would be:  
CN=Jason Sprague,CN=Users,DC=sales,DC=mcmcse,DC=COM

And what about my computer called WOPR? It would be:  
CN=WOPR,CN=Computers,DC=mcmcse,DC=COM

## Authentication

LDAP authentication consists of the following operations:

- **Bind.** Initiates a protocol session to the DSA. After a session is established, a method of authentication is negotiated between the DSA and the client. When the client is authenticated by the DSA, the DSA returns a bind response to the client.
- **Unbind.** Terminates an LDAP session between the client and the DSA.
- **Abandon.** Issued by the client to stop obtaining the results of a previously initiated operation.

## Binding

- Bind initiates a protocol session to the DSA. After a session is established, a method of authentication is negotiated between the DSA and the client. When the client is authenticated by the DSA, the DSA returns a bind response to the client.
- Binding determines at which level a user has rights to. They will have rights for everything at that particular level and below but don't have rights above that value.

## Binding consists of:

- **An LDAP request:** initiates a protocol session to the domain controller. After a session is established, a method of authentication is negotiated between the domain controller and the client. By default, Kerberos is used, but other methods can also be used. Finally, the domain controller returns a bind response to the client when the client is authenticated.
- **Followed by an LDAP bind response:** an indication from the server regarding the status of a request for authentication of the client. If the bind is successful, the result code is "success." Otherwise, an error is reported in accordance with RFC 2251.

## The following is a Network Monitor example of a successful LDAP bind response:

In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory Domain Services object is known as *binding*. When a programmatic object, such as an [IADs](#) or [DirectoryEntry](#) object, is associated with a specific directory object, the programmatic object is considered to be *bound to* the directory object.

**From:** <http://www.faq.nuvotera.com/determine-base-dn-bind-dn-domain-configuring-directory-sync/>

How do I determine the Base DN and Bind DN for a domain configuring Directory Sync?  
Instructions/Procedure:

1. Log in to your Active Directory.
2. Browse to the location of your user accounts.
3. Pick a single user.
4. Have the distinguished name of that user provided.

The distinguished name of a user will also include the Base DN. You simply need to remove the beginning entry in the distinguished name to find the Base DN. Below is an example:

Distinguished Name:

CN=Test User,OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com

#### **Search Base DN:**

OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com

(The Search Base DN tells the server which part of the external directory tree to search)

The Administrator account may not be in the same location as the user accounts. Locate the distinguished name for the Administrator account to find your Bind DN. The Bind DN is the distinguished name of the Administrator account.

Distinguished Name:

CN=Administrator,OU=Admins,OU=Users,DC=corp,DC=yourdomain,DC=com

#### **Search Bind DN:**

CN=Administrator,OU=Admins,OU=Users,DC=corp,DC=yourdomain,DC=com

(The Search Bind DN is the user on the external AD server that is permitted to search the AD directory within the defined search base)

#### **Additional Information**

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. You can use AD Explorer to easily navigate an AD database and identify the Bind and Base DN's as necessary.

#### **Email from Ron Dries (8 Apr 15)**

I jotted down some quick notes to try and remove confusion:

Search Base DN – default base distinguished name to use for searches

Bind DN – Administrator user account on the LDAP server in distinguished name format

Bind Password – Password for the administrator account used for binding

NSS Password – distinguished name format of where on the LDAP server to search for user credentials

#### **Email from Ron Dries (3 Oct 16)**

The **NSS password** is needed even for Windows active directory. This field is just specifying which directory on the Active Directory server to search for user passwords and other attributes needed. This field helps to limit the search and make it more direct. Without it the search can take a very long time, or it could not find the information at all if it hits its search limit before finding what its looking for.

LDAP allows you to use more than one account for logging in. The Bind DN and password are only used to connect to the server and search for users on it.

#### **For example:**

A base DN could be DC=test, DC=com

Bind DN could be CN=Admin, OU=Administrators, DC=test, DC=com

Bind PW could be password: testpassword

The bind user authenticates with the LDAP server, and with the correct permissions is allowed to search for the user credentials that the login was attempted with.

NSS password is a distinguished name of where to look, with a scope. For example OU=Users, OU=Test,?sub which will look in the Test/Users directory for the credentials that were used in the attempted login.

LDAP users all have admin level access. You will be able to configure a group for ldap users.

**Logging in to the Time server using LDAP** – When logging in the time server, the time server will try to bind to the admin account that has been configured using the password that has been configured. If the bind is successful, the LDAP server will search the user list for the username that was typed. If a user is found, it checks the password that was typed. If the password is correct the LDAP server tells the time server that access is granted for that user.

If the bind fails, the database search can't occur. Make sure that the Bind DN can be manually logged into using the configured Bind password. If login isn't possible, this issue has to be addressed in the LDAP server before proceeding.

**Internal use only-** Note that here at the factory, we happen to use the same user login password as the bind

password for our testing. This was just for simplicity as these two passwords are usually different values!!!

## LDAP configuration in the SecureSync

### Desire to pre-configure LDAP settings

**NOTICE:** Users cannot pre-configure LDAP settings before the SecureSync is connected to the network and can reach the LDAP server

**Email from Dave L to Ron Dries** Our customer was having some difficulties getting their LDAP to work. We have these resolved now but now he wants to pre-configure the SecureSync settings and ship to their data centers so they are plug and play.

They are having issues presetting the LDAP configuration. The LDAP configuration will not allow it to save without the LDAP Server being up and reachable at the time of configuration. So it will not allow him to save the configs.

We considered one option of setting it up and then saving a config file. Then loading the config file once its installed at the data center. This is a workaround but may be our only choice to save the LDAP configs.

Do you have any other ideas how they could get this working?

**Reply from Ron Dries (28 Feb 2019)** The LDAP configuration prevents this as a means to make sure that the user does not get locked out of the SecureSync.

Creating a config bundle and applying it to the unit when it is installed in the datacenter would work. Or they can preconfigure the unit except for LDAP then configure just LDAP when it is powered up in the datacenter.

### LDAP config file (ldap.conf)

- Path to ldap.conf config file Spectracom/etc/ and then type **cat ldap.conf**
- Path to LDAP: Spectracom/etc/openldap

### Network ports used with LDAP:

- LDAP port is **389** (and port **636** for SSL when using an SSL certificate)

### LDAP config via CLI

- Not sure what software version these commands were added in.

1. Type **ldap** (followed by the tab key) to view the list of all ldap commands

```
main@spectracom ~$ ldap
ldapadd      ldapdelete  ldapmodify  ldappasswd  ldapurl
ldapcompare  ldapexop    ldapmodrdn  ldapsearch  ldapwhoami
```

### LDAP config via web browser

**Note:** Software update version 5.4.0 removed particular fields from the Active directory/OpenLDAP pages that weren't applicable to this selection (such as NSS only applies to Active Directory, but it was displayed in when OpenLDAP was selected)

**Note:** software update version 5.2.0 improved LDAP Configuration status reporting in the browser

### Five tabs for LDAP setup

- **Settings:** This is where you set up the general LDAP Distinguished Name and Bind settings.
- **Security:** This is where you upload and manage the CA server certificate, CA client certificate and CA client key.
- **Group:** This is where you enable/disable group-based authentication.
- **Advanced:** This is where you set up your search filter(s) and login attribute.
- **Servers:** This is where you identify the LDAP server to be used.

**Management -> Authentication** page of the browser. Click "**LDAP Setup**" on the left side of the page

## 1. Settings tab

**Classic interface, version 5.4.1 software installed**

LDAP SETUP

General Settings | LDAP Servers Configuration | SS Authentication | Group Authentication

### LDAP Settings

|                                    |                                  |
|------------------------------------|----------------------------------|
| LDAP Server Type                   | Active Directory on Windows Serv |
| Port for server binding            | 389                              |
| Time limit for searching (seconds) | 120                              |
| Time limit for binding (seconds)   | 120                              |
| LDAP protocol version              | LDAPv3                           |
| Scope to search server with        | Sub                              |

There must be at least one saved LDAP server in order to configure the above settings.

### LDAP Services

|                        |          |
|------------------------|----------|
| Console Login / Telnet | Disabled |
| FTP                    | Disabled |
| SSH / SFTP / SCP       | Disabled |
| HTTP / HTTPS           | Disabled |

Submit Reset

**LDAP Services:** Classic browser allows individual enable/disable of CLI, Browser FTP, etc. Newer blak/charcoal browser doesn't provide this capability (though these ealier configs in the classic browser still apply).



## New browser with v5.5.1

LDAP Setup

Settings Security Group Advanced Servers

Enabled

Server Type: Active Directory

Search Base DN: dc=int,dc=orolia,dc=com

Bind DN: CN=ldaptest,OU=ROC-IT User:

Bind Password: .....

NSS Base: OU=ROC-IT,OU=ROC,?sub

Port: 389

Auto-follow Referrals

Submit

**Port** field: wasn't available in versions 5.4.1 and below. Is available in at least versions 5.5.1 and above.



**LDAP Setup**

Settings Security Group Advanced Servers

Enabled

Server Type: Active Directory

Search Base DN: dc=int,dc=orolia,dc=com

Bind DN: CN=ldaptest,OU=ROC-IT Use

Bind Password: [masked]

NSS Password: [masked]

Auto-follow Referrals

**“Search Type” field**  
Active Directory: For Windows  
Open LDAP: For Linux

**Search Base DN (Domain Name):** The Search Base DN tells the server which part of the external directory tree to search. (example for us “.int.orolia.com”)  
You simply need to remove the beginning entry in the Distinguished Name to find the Base DN. Below is an example:  
**Distinguished Name:** CN=Test User,OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com  
**Base DN:** OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com

**Bind Password**  
Note: “Bind DN” and “Bind Password” are “paired”  
The Active Directory password for the account that can search for users.  
**Note:** The Bind password is the same password used in association with the Bind DN user account.

**Bind DN**  
Note: “Bind DN” and Bind Password are “paired”  
The Search Bind DN is the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users.  
Locate the distinguished name for the Administrator account to find your Bind DN. The Bind DN is the distinguished name of the Administrator account.  
Distinguished Name:  
CN=Administrator,OU=Admins,OU=Users,DC=corp,DC=yourdomain,DC=com  
Bind DN:  
CN=Administrator,OU=Admins,OU=Users,DC=corp,DC=yourdomain,DC=com

**NSS Password**  
Note: this field required- it can't be left blank. See additional info further below  
Only displayed when the “Server Type” field (in the “Settings” tab) is set to “Active Directory”. This field is mandatory when displayed.

**Note:** Bind DN / Bind Password may not accept certain special characters.

**JIRA-SSS-682 (created 27 Aug KW) for insecure storage of Bind password:** Per Salesforce case 203529 (7/19/2019) the State of Tennessee is using LDAP and is asking us if the bind password can be stored in a different way, instead of plain text. They are making a feature request due to security concerns about the PW being stored this way.

### Search base DN field in new browser

**This field is too restrictive with rules (5.5.1 and below):**

**(email from, Dave L on 24 Mar 17)** There is a limitation in the web browser when configuring LDAP. The Search Base DN and some other fields are too restrictive to what characters can be used. In this case we recommend using the “Classic” interface to setup LDAP. The Classic web UI does not have these restrictions. This is still an issue in version 5.5.1. We have addressed this in the new firmware release but it will be a few weeks until this is available to the general public. Please use the Classic UI for now.

### NSS password field

**Example of an NSS password** ROC-IT,OU=ROC,?sub

**Note:** “NSS Password” allows administrators to specify a list of sources where authentication files, host names and other information will be stored and searched for in the AD server.

This is not really a “password” (the word ‘password’ is associated with the unix ‘password’ directory, where user accounts are stored in unix). This field defines the path to the closest directory containing all of the users with unix (GID) attributes you wish to be able to login to the SecureSyncs (shortest path possible, but high enough to be able to include all desired users)

## Windows Active Directory/ Group policy / LDAP

- Refer to: <http://social.technet.microsoft.com/Forums/windowsserver/en-US/cff39c31-b82b-4e69-babb-9dd94caa0267/ldap-client?forum=winserverGP> (Info for Server 2003, Server 2008. Server 2012)

**Note:** For simplicity, think of “**Active Directory**” as being the “LDAP server for Windows”. The two choices for LDAP configurations is either **Active Directory** (for Windows) or “**Open LDAP**” (for Linux). These are essentially treated similarly but changes the configs in the SecureSync.

**Active Directory (AD)** is a [directory service](#) that [Microsoft](#) developed for [Windows domain](#) networks and is included in most [Windows Server](#) operating systems as a set of [processes](#) and [services](#).<sup>[1][2]</sup> An AD [domain controller authenticates](#) and [authorizes](#) all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user [logs into](#) a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a [system administrator](#) or normal user.<sup>[3]</sup> Active Directory makes use of [Lightweight Directory Access Protocol](#) (LDAP) versions 2 and 3, Microsoft's version of [Kerberos](#), and [DNS](#).

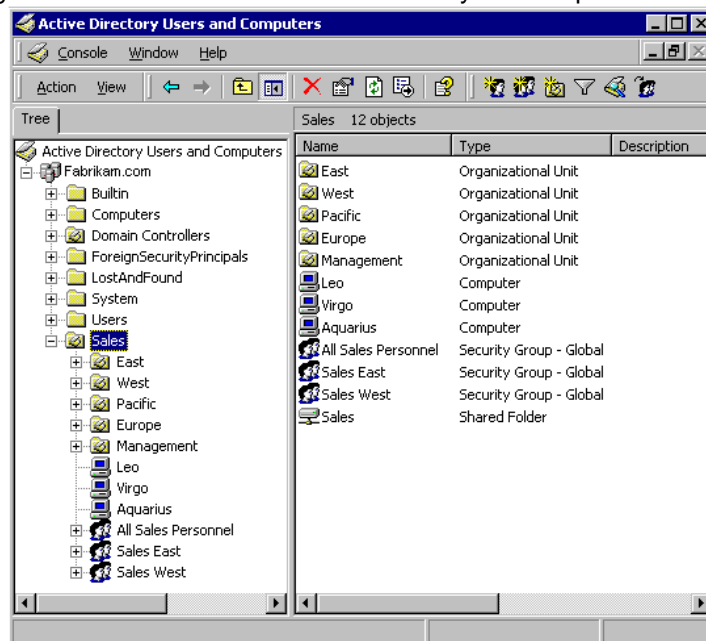
**Below is from:** <https://msdn.microsoft.com/en-us/library/aa746492%28v=vs.85%29.aspx>

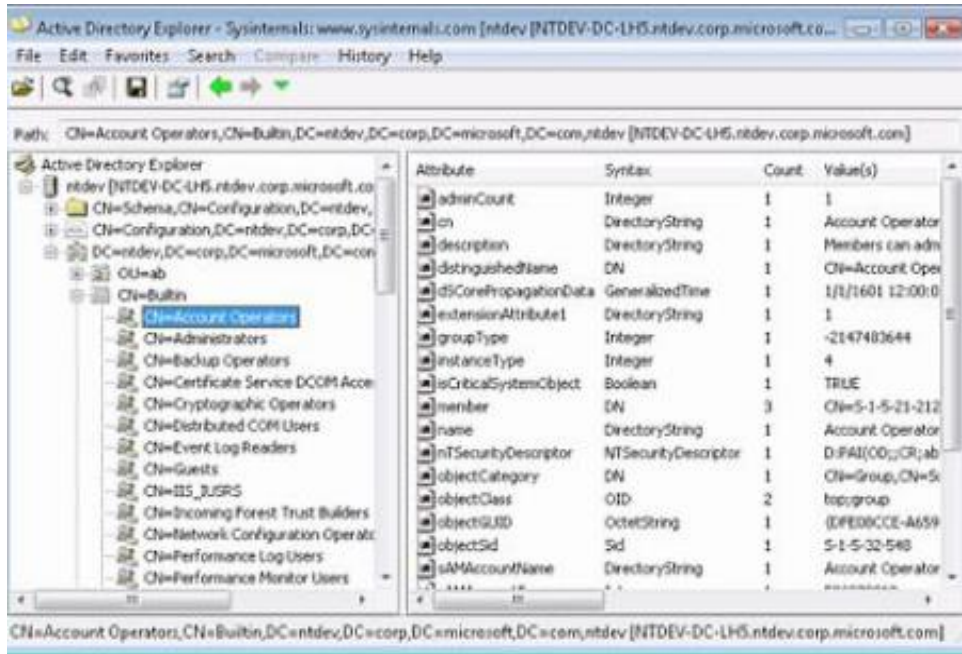
Active Directory is a special-purpose database. The directory is designed to handle a large number of read and search operations and a significantly smaller number of changes and updates. Active Directory data is hierarchical, replicated, and extensible. Because it is replicated, you do not want to store dynamic data, such as corporate stock prices or CPU performance. If your data is machine-specific, store the data in the registry.

Typical examples of data stored in the directory include printer queue data, user contact data, and network/computer configuration data. The Active Directory database consists of objects and attributes. Objects and attribute definitions are stored in the Active Directory schema.

You may be wondering what objects are currently stored in Active Directory. In Windows 2000, Active Directory has three partitions. These are also known as naming contexts: domain, schema, and configuration. The domain partition contains users, groups, contacts, computers, organizational units, and many other object types. Because Active Directory is extensible, you can also add your own classes and/or attributes. The schema partition contains classes and attribute definitions. The configuration partition includes configuration data for services, partitions, and sites.

The following screen shot shows the Active Directory domain partition.





Below info is from: <http://msdn.microsoft.com/en-us/library/ff632147.aspx>

**The server activities are as follows:**

- Upon receiving an LDAP bind request ([RFC2251] section 4.2, Bind Operation) from the Client Application, the directory server interacts with the Microsoft Windows® Authentication Services which authenticates the Administrator using the supplied credentials ([MS-AUTHSO] section 4, Interactive Domain Logon Task).
- The directory server receives the LDAP add request, containing data about the new user object to be created. The directory server validates that the Administrator has the necessary access to perform the operation. If the Administrator does not have the necessary access to perform the operation, the directory server rejects the LDAP add request.
- The directory server verifies the constraints for add operations are satisfied as outlined in [MS-ADTS] sections 3.1.1.5.1, General, and 3.1.1.5.2, Add Operation. If the constraints are not satisfied the add request will be terminated with an appropriate error.
- Additional constraints specific to account creation are validated as outlined in [MS-SAMR] section 3.1.1.6, Attribute Constraints for Originating Updates. If the constraints are not satisfied, the add request will be terminated with an appropriate error.
- The user object is created in the directory and populated with the data supplied in the request. Additional attributes on the object are populated based on the server's processing rules as outlined in [MS-ADTS] section 3.1.1.5.2.4, Processing Specifics, and [MS-SAMR] section 3.1.1.8, Attribute Triggers for Originating Updates.
- The directory server receives password information from the KDC. The password is set to the supplied value.
- The directory server receives LDAP modify requests containing new values for the userAccountControl and pwdLastSet attributes. The attributes are updated with the supplied values.

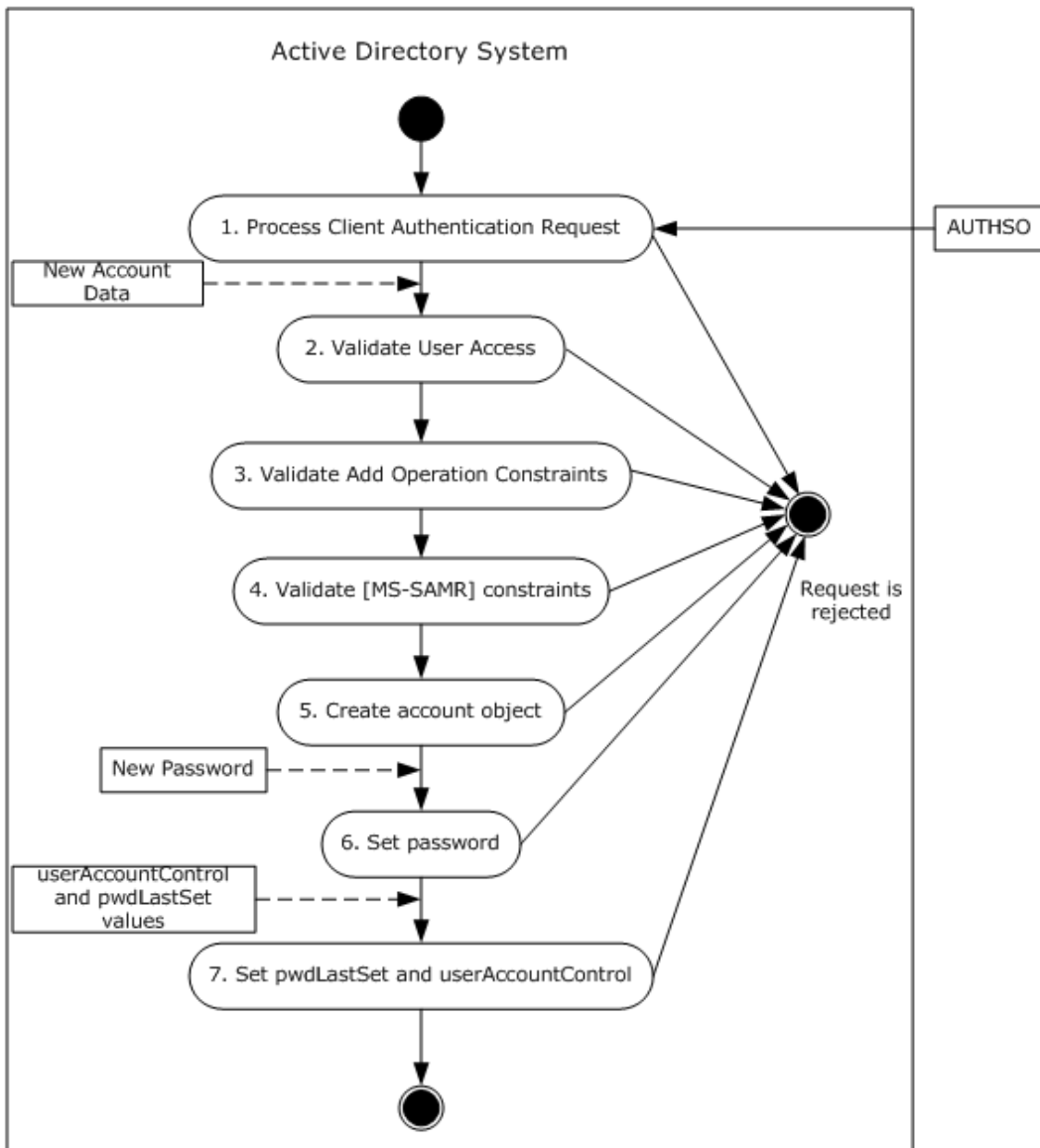
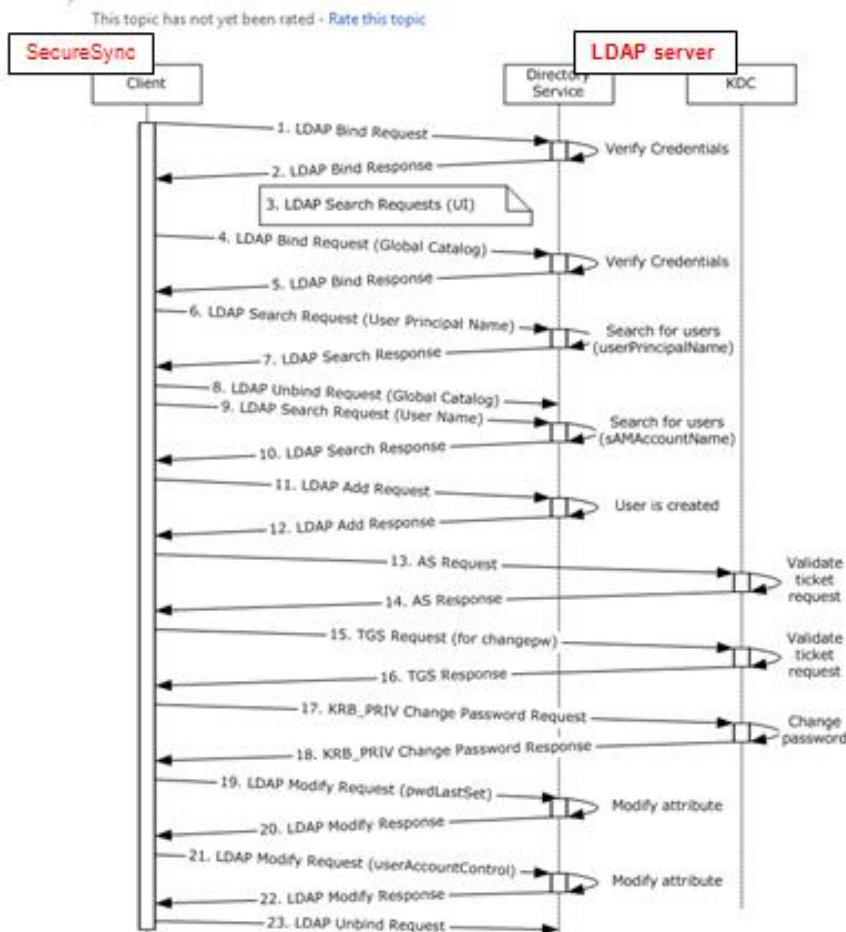


Figure 23: Server activity diagram for provisioning a user account using the LDAP protocol

## Connection

## 6.1.1.3 Sequence of Events



Unless otherwise noted, all responses that include a return code contain a return code indicating that the operation was successfully performed.

1. The program (see section 6.1.1) establishes an [LDAP](#) connection to the [directory](#) server. An **LDAP bind request** ([RFC2251](#) section 4.2, Bind Operation) is sent to the directory server with the credentials of an administrator.
2. The directory server uses one of the methods defined elsewhere (see [\[MS-AUTHSO\]](#) section 4, Interactive Domain Logon Task) to verify the credentials. Depending on the negotiated authentication method, this may involve additional client and server interactions not directly relevant here. After that verification, the directory server sends an **LDAP bind response** ([RFC2251](#) section 4.2.3, Bind Response) to the client.
3. At this point the client sends **LDAP search requests** ([RFC2251](#) section 4.5.1, Search Request) to populate data in the tool's user interface. This step is necessary only for user-interface display purposes specific to the example shown in the figure captioned, "Message flow for provisioning a user account using the LDAP protocol".
4. An LDAP connection to a [global catalog](#) is established. An **LDAP bind request** ([RFC2251](#) section 4.2, Bind Operation) to the global catalog is sent with the administrator's credentials.
5. The global catalog verifies the credentials ([\[MS-AUTHSO\]](#) section 4, Interactive Domain Logon Task) and sends an **LDAP bind response** ([RFC2251](#) section 4.2.3, Bind Response).
6. An **LDAP search request** ([RFC2251](#) section 4.5.1, Search Request) is sent to the global catalog, querying the entire [forest](#), starting at the root of the forest, looking for [security principals](#) that have the same [user principal name](#) as the requested user principal name of the new [account](#), to verify that the requested user principal name of the new account is not currently in use.
7. The global catalog sends an **LDAP search response** ([RFC2251](#) section 4.5.2, Search Result) listing any accounts that have the user principal name specified.
8. An **LDAP unbind request** ([RFC2251](#) section 4.3, Unbind Operation) is sent to the global catalog. The LDAP connection to the global catalog is closed.

9. The program sends an **LDAP search request** ([\[RFC2251\]](#) section 4.5.1, Search Request) to the directory, querying the entire **domain**, starting at the root of the domain, looking for security principals that have the same name (stored in the sAMAccountName attribute) as the one requested for the new account, to ensure that the name specified by the administrator is not currently in use.

10. The server sends an **LDAP search response** ([\[RFC2251\]](#) section 4.5.2, Search Result) listing any accounts that have the user name specified.

For the purposes of this scenario, assume that the LDAP search responses for the user principal name and the account name do not contain any accounts, that is, there were no matches. The program has now verified that the user principal name and user name chosen are not currently in use and continues with the add operation.

11. An **LDAP add request** ([\[RFC2251\]](#) section 4.7, Add Operation) is sent to the server. The LDAP add operation contains the distinguishedName, sAMAccountName, userPrincipalName, displayName, and givenName of the new user, and specifies that the **object class** of the object to be created is user.

12. The server processes the add request ([\[RFC2251\]](#) section 4.7, Add Operation) and performs validation as described in [\[MS-ADTS\]](#) sections [3.1.1.5.1](#), General, and [3.1.1.5.2](#), Add Operation. It then sends an **LDAP add response** indicating success.

Now that the user has been created, the program starts setting additional **attributes** provided by the administrator. It begins by setting the password for the new account. This is done via **Kerberos** messages sent to the Kerberos **Key Distribution Center (KDC)**.

13. The client begins by sending a Kerberos **AS** request ([\[RFC4120\]](#) section 3.1, The Authentication Service Exchange) to the Authentication Service (AS) requesting a **Ticket-Granting Ticket (TGT)** that it will use for later authentication.

14. The service validates the credentials ([\[MS-AUTHSO\]](#) section 4, Interactive Domain Logon Task) in the AS request and sends an AS response ([\[RFC4120\]](#) section 3.1, The Authentication Service Exchange) with a TGT.

15. The client sends a Kerberos **TGS** ([\[RFC4120\]](#) section 3.3, The Ticket-Granting Service (TGS) Exchange) request to the Ticket-Granting Service (TGS) using the TGT and requesting a **service ticket** for the kadmin/changepw service ([\[RFC3244\]](#)), which provides functionality to change an account's password via Kerberos.

16. The service validates the credentials in the TGS request and sends a TGS response ([\[RFC4120\]](#) section 3.3, The Ticket-Granting Service (TGS) Exchange) with the service ticket.

17. Using the service ticket, the client sends a **KRB\_PRIV** change password request ([\[RFC4120\]](#) section 3.5, The KRB\_PRIV Exchange, and [\[RFC3244\]](#) section 2, The Protocol) to the Kerberos password-changing service with the new password for the account.

18. The password-changing service processes the request and sends a KRB\_PRIV response ([\[RFC4120\]](#) section 3.5, The KRB\_PRIV Exchange, and [\[RFC3244\]](#) section 2, The Protocol) indicating success. As part of this change-password operation, the Active Directory database is modified according to the sequence of actions described in [\[MS-SAMR\]](#) section [3.1.1.8.5](#), clearTextPassword.

At this point the Kerberos operations are completed. The client now continues to set remaining attributes via LDAP.

19. If the administrator indicated that the user must change his or her password at next logon, the client sends an LDAP modify request ([\[RFC2251\]](#) section 4.6, Modify Operation) setting the pwdLastSet attribute to 0. This setting tells the server that the user's password has expired and must be changed the next time the new user attempts to log on.

20. The server processes the request and sends a response ([\[RFC2251\]](#) section 4.6, Modify Operation). The client computes the new desired value for the userAccountControl attribute. At a minimum this includes the ADS\_UF\_NORMAL\_ACCOUNT bit ([\[MS-ADTS\]](#) section [2.2.15](#), userAccountControl Bits) and may contain additional bits depending on administrator-provided values.

21. The client sends an LDAP modify request ([\[RFC2251\]](#) section 4.6, Modify Operation) with the new value for userAccountControl.

22. The server processes the request and sends a response ([\[RFC2251\]](#) section 4.6, Modify Operation). The new user account (represented as a **directory object** of class user) has now been created. The user object has been populated with all specified attributes.

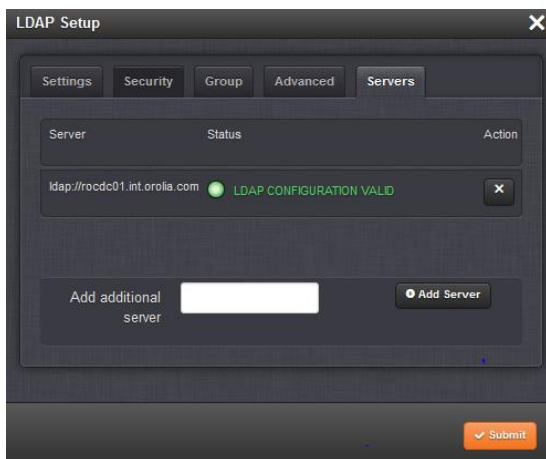
23. The client sends an LDAP unbind request ([\[RFC2251\]](#) section 4.3, Unbind Operation) to the server. The LDAP connection to the directory server is closed.

- Was added to the bottom of the “**Settings**” tab (I believe in version 5.2.0)
- For more info on referrals, refer to: <https://technet.microsoft.com/en-us/library/cc978014.aspx> and <https://technet.microsoft.com/en-us/library/cc978014.aspx>

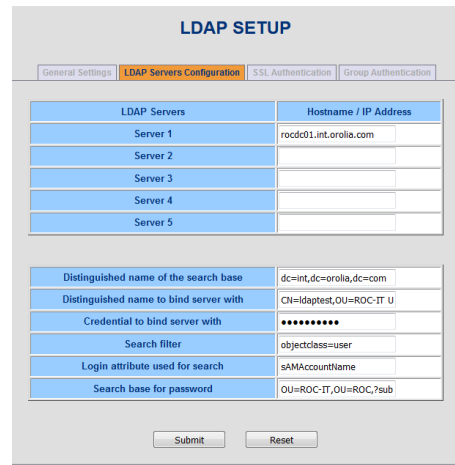
An LDAP referral is a domain controller's way of indicating to a client application that it does not have a copy of a requested object (or, more precisely, that it does not hold the section of the directory tree where that object would be, if in fact it exists) and giving the client a location that is more likely to hold the object, which the client uses as the basis for a DNS **search for a domain controller**.

To make use of cross-references, clients must be enabled to follow ("chase") referrals that are returned. Windows Address Book chases referrals by default. In LDAP, you can specify **Chase Referrals** in the search options. When you are using ADSI programmatically (for example, by using Active Data Objects [ADO] to search), you must specify whether to chase referrals.

## 2. Servers tab



classic interface (5.4.1 software installed)

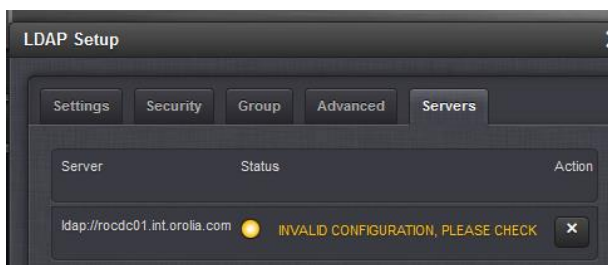


### Number of LDAP servers that can be listed

**Email from Dave L (20 Jan 17)** I am not sure exactly what the limit of the number of LDAP Servers you can enter is but it is over 10. The number of LDAP Servers you configure depends on how many you have available and where they are located. I do not think more than two is necessary.

If more than one LDAP Server is configured and is not available, the login will be delayed while the Securesync tries to establish communications with each one of the LDAP Servers. The delay depends on the timeout and number of retries. The local login will not occur until all the LDAP Servers have been contacted or timed out. So please make sure you enter LDAP Servers that will always be reachable.

**“Invalid configuration, please check”** displayed, after entering LDAP server’s address



- 1) Make sure the Primary DNS /Secondary DNS server addresses are correct in the Ethernet interface settings. If DNS settings are missing or incorrect, this will occur.
- 2) Must use URI format for the LDAP address (“LDAP://” in front of the address- not LDAP:\)

- Must use URI format (refer to: [https://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol#URI\\_scheme](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#URI_scheme))

**Important Note about URI format:** whether configuring the LDAP sever using its IP address or its hostname, this value MUST use **URI** format (value must always begin with the following: **ldap://** (not **ldap:\**))

**Examples:** [ldap://10.1.1.1](#) or [ldap://Microsoft.com](#)

Enter the hostname or IP address of the LDAP server and then press “**Add Server**”

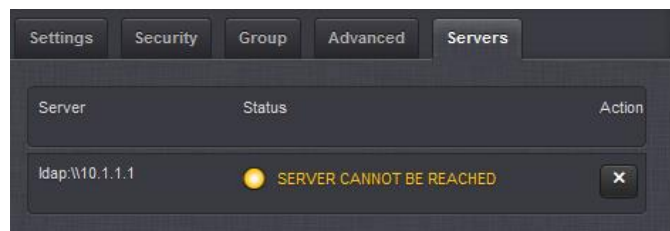
Version 5.2.0 Improved add/delete of LDAP servers.

### LDAP Server Status

- Only displayed if at least one LDAP server has been added.
- SecureSync pings the configured server to see if its reachable on the network.
- Mantis case 2834 (software versions 5.1.4 and 5.1.5): “LDAP Servers status” reports “Configuration missing” even though LDAP is working just fine (“Servers Status” was improved in version 5.2.0)

### Displays one of the following states:

- **PASS (green):** indicates LDAP configuration is valid, An LDAP server that has been set up is available and is able to pass data. The configured LDAP server is responding to ping (reachable on the network)
- **Server cannot be reached (orange/yellow)**



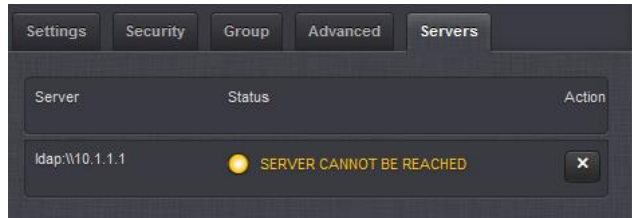
- **CONFIGURATION MISSING (red):** No configuration files are available.  
LDAP may not be configured in SecureSync or software versions 5.1.4 or 5.1.5 installed (refer to “Mantis case 2834” note above)
- **FAILED TO READ DATA (red):** An LDAP server is available but no data was passed.
- **FAILED NOT REACHABLE (red):** No LDAP server could be reached.
- **LDAP DISABLED:** The Enabled checkbox under the Settings tab as not been selected. (LDAP not Enabled in the Settings tab).
- **“INVALID CONFIGURATION”:** whether configuring the LDAP sever using its IP address or its hostname, this value **MUST** use **URI** format (value must always begin with the following: “**ldap://**”

**Examples:** [ldap://10.1.1.1](#) or [ldap://Microsoft.com](#)

**Note:** After entering the LDAP server address, if the “**Servers**” tab reports “**server cannot be reached**”



(instead of “LDAP Configuration valid”)



### Verify:

- 1) Whether using the LDAP server's IP address or hostname, the Server line must begin with **ldap://** (and not “ldap:\\”)
  - Example above shows the wack/wack going in the wrong direction (instead of \\, it should be //)
- 2) (if using a hostname instead of IP address) DNS is configured correctly and working (try temporarily using its IP address to see if it then connects. If it does, there is a DNS-related issue.
- 3) make sure all the LDAP settings (in the Settings tab) are correct. these do affect the adding of a server.

---

### Software update version 5.2.0

- Improved LDAP Configuration status reporting in the web browser.
- Improved add/delete of LDAP servers.
- Improvements to LDAP group authentication.
- Removed password expired message (LDAP/RADIUS only) that was displayed when logging in as a remote user.

---

### LDAP allows more than one account for logging in

- LDAP allows you to use more than one account for logging in. The Bind DN and password are only used to connect to the server and search for users on it.

---

### \*\*\*Login access levels (permissions/rights)

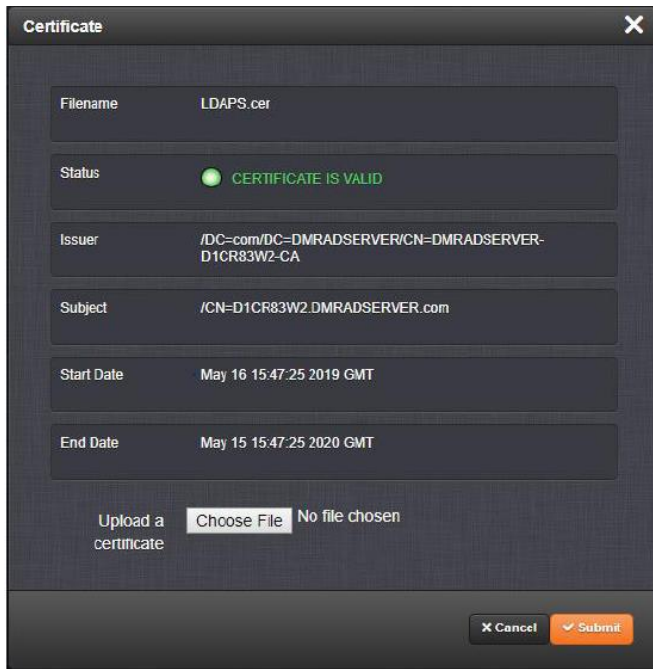
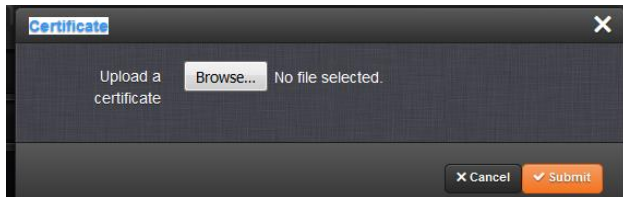
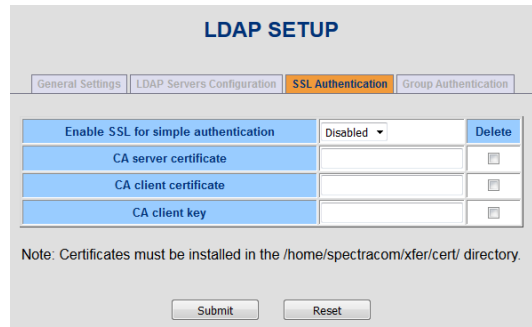
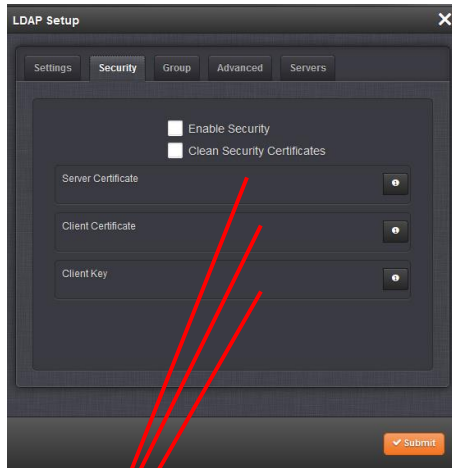
- In at least software versions 5.2.0 and below, all authorized LDAP users automatically have admin rights.
  - There is no way to differentiate between admin (Read/Write- “RW”) and user rights (Read Only - “RO”)

---

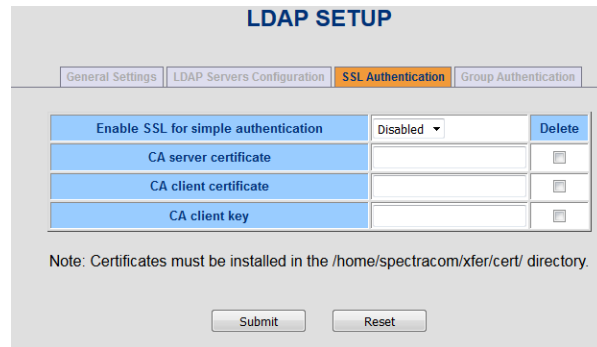
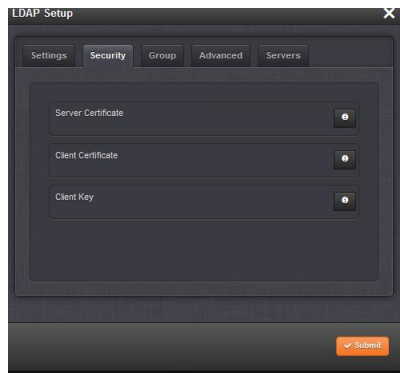
#### 1. Security tab (SSL certificate for LDAPS-LDAP secure)

- **Software Update Version 5.5.0:** “Corrected defects in LDAP Security configuration in Web UI and in Classic Web UI.”

#### A) Version 5.5.0 and above screenshots



## B) Version 5.4.1 screenshots



---

### “Unrecognized Certificate format”

- Refer to case 195461
- It appears that LDAP needs to be configured for the LDAP certificate to be visible.

**Customer Report:** I tried loading this certificate into a Securesync with both v5.7.1 and 5.8.4 firmware. The certificate was not accepted into either. I have forwarded your information on to our Applications Engineers for comment. They may be able to identify the problem.

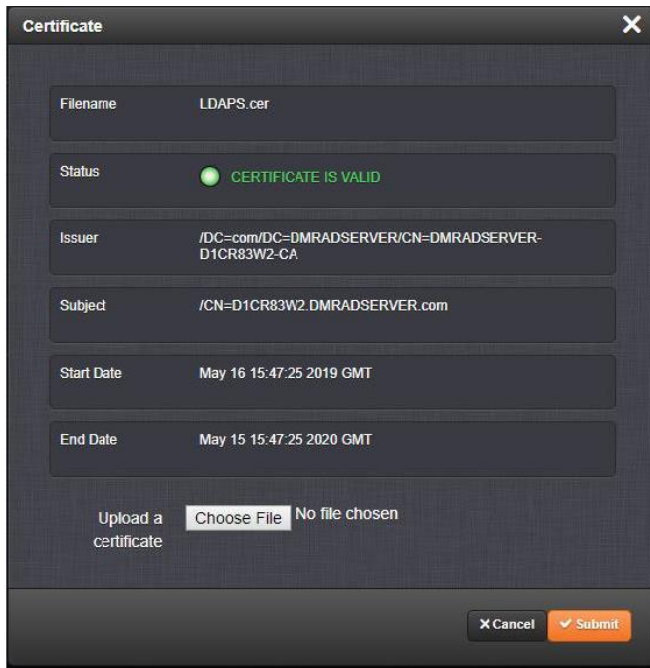
There seems to be a problem with the certificate being accepted by the Securesync. This is probably due to the certificate itself. I believe Keith sent you the LDAP/Radius Application note. There are instructions starting on page 12 for uploading the Server Certificate.

When you exported the certificate from the LDAP Server were any particular options selected? Please try exporting a new certificate and loading it into the Securesync.

I also recall you mentioned these were issues with Firefox and the Securesync so I tested the Securesync HTTPS connection with the current version of Firefox using the Firefox self signed certificate and it works fine. No problems opening the web browser.

**A reply from Dave L (17 May 2019)** I consulted out Applications Engineer and he discovered the issue. He was able to upload the certificate to the SecureSync, It appears that LDAP needs to be configured for the certificate to be visible.

The certificate needs to be renamed for it to work. He renamed it to LDAPS.cer and it is now readable. He had the same error as you reported when it is named LDAS certificate.cer

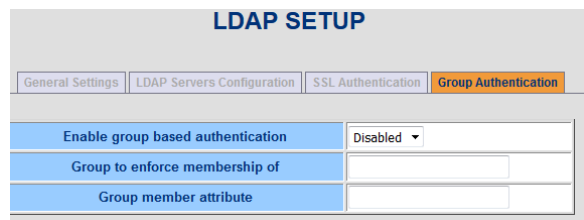
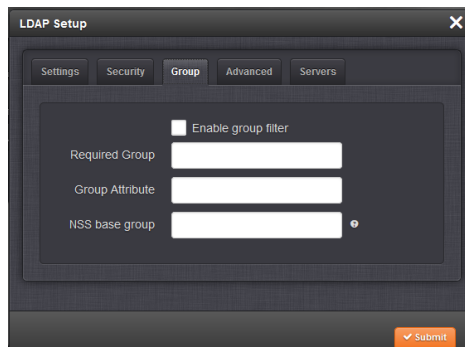


I hope this resolves your problem. Please try renaming and let me know how it goes.

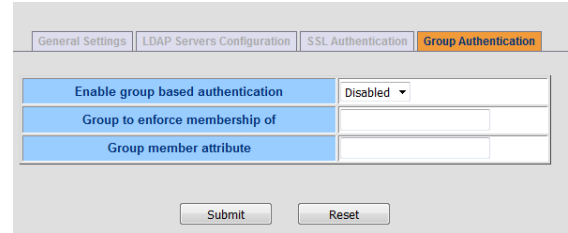
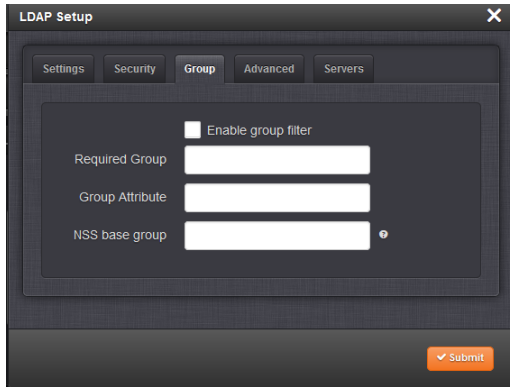
## 2. Group Tab (to apply an LDAP Group Filter)

**Function:** Groups are a quick way of giving users common access to certain features or functionality within an LDAP directory.

### A) Version 5.5.0 and above screenshots

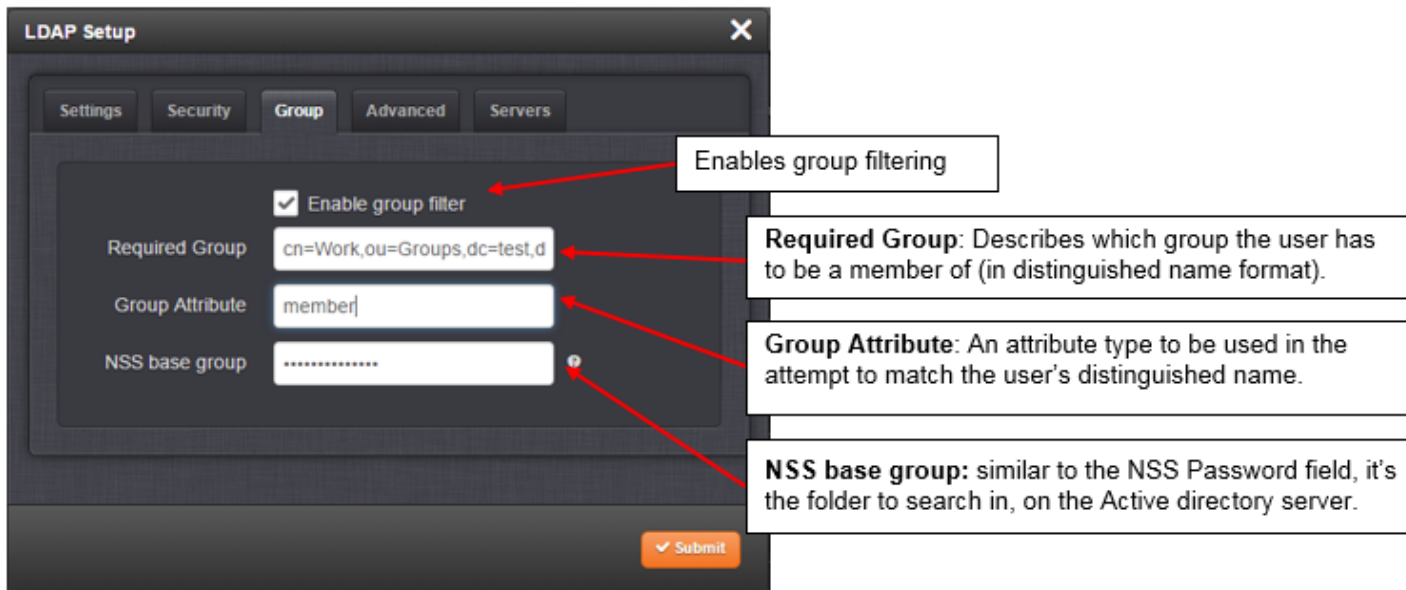


### B) Version 5.4.1 screenshots



- Software Update version 5.2.0 incorporated changes to LDAP group. (Refer to Mantis Case 2960:
  - **From the v5.2.0 Release Notes:** “Improvements to **LDAP group authentication**, addressing reported login issue.”
    - The group distinguished name field was too short to accept the groupdn for the ROC spectracom groups distinguished name
    - When user was not in the group specified ssh and telnet would alert that you must be in the group but still log you in
    - When Radius and LDAP were both enabled at the same time, the UI would allow access even if the user was not in the specified LDAP group
- In at least versions 5.1.7 and below, group filter can only be configured via the web browser.

**Email from Ron Dries (12 Jan 2015) regarding Salesforce case 16840** So I'm not entirely sure if this will work for their setup, but it's currently how I believe group authentication with LDAP works now in the SecureSync.



The above image is the group filter configuration tab for LDAP.

- The “**Enable Group filter**” checkbox enables group filtering

- The **“Required Group”** field describes which group the user has to be a member of (in distinguished name format). In the above example it’s the group “Work” in the “Groups” organizational unit
- The **“Group attribute”** field is an attribute type to be used in the attempt to match the user’s distinguished name. In the above example, ldap will search the values of the member attribute of the work group looking to see if the user’s “distinguished name” is listed.
- The **“NSS Base group”** field is similar to the NSS Password field. It’s the folder to search in, on the Active directory server.

I believe that the Required Group and NSS base group fields they have, I’m not sure if they have an attribute on the group which can be used to determine if the user’s distinguished name is a member of the group or not.

#### **AD has to support RFC 2307???? (not yet confirmed)**

**Note from keith (7 Mar 17) I BELIVE the Active Directory’s schema must be configured to support RFC 2307 in order to be able to define unix client attributes. Refer to info on “Winbind” with sites such as: [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/7/html/Windows\\_Integration\\_Guide/winbind.html#samba](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/winbind.html#samba)**

---

#### **Expert mode for LDAP Group**

Currently the GUI is the only method of configuring LDAP on the SecureSync; there is no expert mode for this feature.

#### **Known issues with group authentication (v5.1.7 and below. Should be fixed in 5.2.0)**

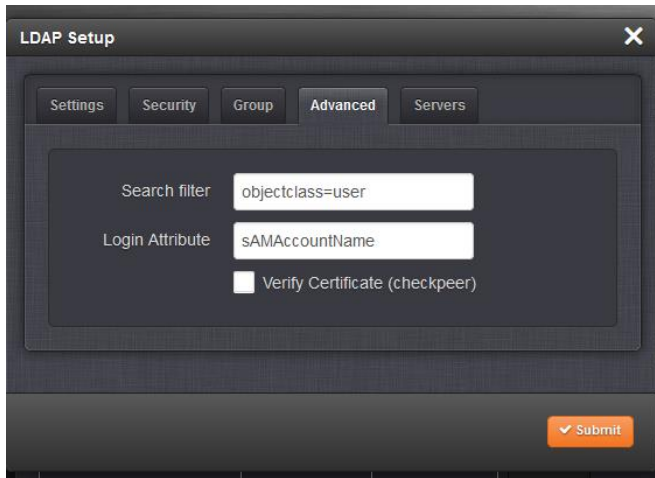
- Refer to Mantis Case 2960 <http://cvsmantis.int.rolia.com/mantis/view.php?id=2960>
  1. The group distinguished name field was too short to accept the groupdn for the ROC spectracom groups distinguished name.
  2. When user was not in the group specified ssh and telnet would alert that you must be in the group but still log you in.
  3. When Radius and LDAP were both enabled at the same time, the UI would allow access even if the user was not in the specified LDAP group

#### **“Group filter” being enabled can cause very long delays in logging in (like 20 minutes for instance)**

Having the group filter enabled (“groups enabled”) can significantly increase the time it takes to authenticate/login (one customer reported it took 20 minutes to login).Disable this checkbox and see if the time it takes to login goes way down. If it does, the SecureSync having to search all of the groups is the reason for the long delay in logging in.

---

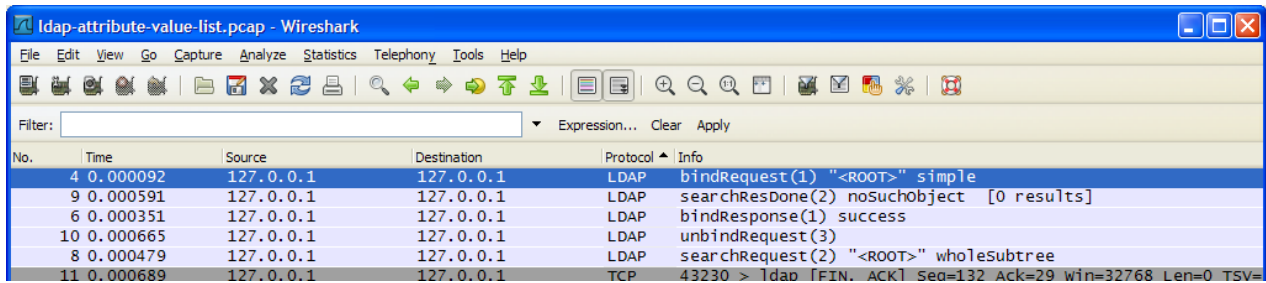
### 3. Advanced Tab (“Search filter” and “Login Attribute”)



The image shows a screenshot of the 'LDAP Setup' dialog box, specifically the 'Advanced' tab. The dialog has a dark grey background and a title bar with 'LDAP Setup' and a close button. Below the title bar are five tabs: 'Settings', 'Security', 'Group', 'Advanced', and 'Servers'. The 'Advanced' tab is selected. Inside the tab, there are two text input fields: 'Search filter' with the value 'objectclass=user' and 'Login Attribute' with the value 'sAMAccountName'. Below these fields is a checkbox labeled 'Verify Certificate (checkpeer)' which is currently unchecked. At the bottom right of the dialog is an orange 'Submit' button with a checkmark icon.

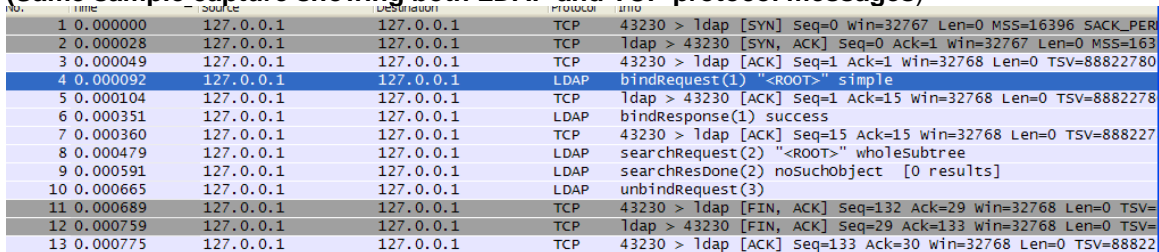
## Packet capture analysis

- **Sample LDAP Packet captures:** Refer to <http://wiki.wireshark.org/SampleCaptures>
- **Sample LDAP packet capture** (showing only LDAP protocol messages)



| No. | Time     | Source    | Destination | Protocol | Info                                                        |
|-----|----------|-----------|-------------|----------|-------------------------------------------------------------|
| 4   | 0.000092 | 127.0.0.1 | 127.0.0.1   | LDAP     | bindRequest(1) "<ROOT>" simple                              |
| 9   | 0.000591 | 127.0.0.1 | 127.0.0.1   | LDAP     | searchResDone(2) noSuchObject [0 results]                   |
| 6   | 0.000351 | 127.0.0.1 | 127.0.0.1   | LDAP     | bindResponse(1) success                                     |
| 10  | 0.000665 | 127.0.0.1 | 127.0.0.1   | LDAP     | unbindRequest(3)                                            |
| 8   | 0.000479 | 127.0.0.1 | 127.0.0.1   | LDAP     | searchRequest(2) "<ROOT>" wholeSubtree                      |
| 11  | 0.000689 | 127.0.0.1 | 127.0.0.1   | TCP      | 43230 > ldap [FIN, ACK] Seq=132 Ack=29 Win=32768 Len=0 TSV= |

### (Same sample capture showing both LDAP and TCP protocol messages)



| No. | Time     | Source    | Destination | Protocol | Info                                                        |
|-----|----------|-----------|-------------|----------|-------------------------------------------------------------|
| 1   | 0.000000 | 127.0.0.1 | 127.0.0.1   | TCP      | 43230 > ldap [SYN] Seq=0 win=32767 Len=0 MSS=16396 SACK_PER |
| 2   | 0.000028 | 127.0.0.1 | 127.0.0.1   | TCP      | ldap > 43230 [SYN, ACK] Seq=0 Ack=1 win=32767 Len=0 MSS=163 |
| 3   | 0.000049 | 127.0.0.1 | 127.0.0.1   | TCP      | 43230 > ldap [ACK] Seq=1 Ack=1 win=32768 Len=0 TSV=88822780 |
| 4   | 0.000092 | 127.0.0.1 | 127.0.0.1   | LDAP     | bindRequest(1) "<ROOT>" simple                              |
| 5   | 0.000104 | 127.0.0.1 | 127.0.0.1   | TCP      | ldap > 43230 [ACK] Seq=1 Ack=15 win=32768 Len=0 TSV=8882278 |
| 6   | 0.000351 | 127.0.0.1 | 127.0.0.1   | LDAP     | bindResponse(1) success                                     |
| 7   | 0.000360 | 127.0.0.1 | 127.0.0.1   | TCP      | 43230 > ldap [ACK] Seq=15 Ack=15 win=32768 Len=0 TSV=888227 |
| 8   | 0.000479 | 127.0.0.1 | 127.0.0.1   | LDAP     | searchRequest(2) "<ROOT>" wholeSubtree                      |
| 9   | 0.000591 | 127.0.0.1 | 127.0.0.1   | LDAP     | searchResDone(2) noSuchObject [0 results]                   |
| 10  | 0.000665 | 127.0.0.1 | 127.0.0.1   | LDAP     | unbindRequest(3)                                            |
| 11  | 0.000689 | 127.0.0.1 | 127.0.0.1   | TCP      | 43230 > ldap [FIN, ACK] Seq=132 Ack=29 win=32768 Len=0 TSV= |
| 12  | 0.000759 | 127.0.0.1 | 127.0.0.1   | TCP      | ldap > 43230 [FIN, ACK] Seq=29 Ack=133 win=32768 Len=0 TSV= |
| 13  | 0.000775 | 127.0.0.1 | 127.0.0.1   | TCP      | 43230 > ldap [ACK] Seq=133 Ack=30 win=32768 Len=0 TSV=88822 |

## Understanding LDAP traffic

When you look at the Info column, you will see several different types data.

- **bindRequest()** This to be authentication request from us to the ldap server
- **bindResponse()** This is the response from the ldap server (domain controller) in response to our bindRequest().
- **SASL GSS-API Integrity: searchRequest()** This is a request to the ldap server. If you look in the middle pane of Wireshark, you will see a collapsed section called *Lightweight-Directory-Access-Protocol | SASL Buffer | GSS-API payload | LDAPMessage searchRequest()*. Here you will see specifics of what you are requesting from the ldap server. In particular, you can drill down to *protocolOp: searchRequest()*. Here you can see the *Filter* (this is the actual ldap query sent) that was used. You can also see the *attributes* that were requested. You can also see the *baseObject* here.

In terms of SQL, this is basically like the select statement.

- **Filter = SQL where clause**  
**attributes = SQL list of columns to select**  
**baseObject = roughly translates to a SQL table, but more just specifying at what level in the ldap tree the search should take place.**

### SASL GSS-API Integrity: searchResEntry()

This is the response to the *searchRequest()* request from the ldap server. If you look in the middle pane of Wireshark, you will see a collapsed section (unless you already opened it :) called *Lightweight-Directory-Access-Protocol | SASL Buffer | GSS-API payload | LDAPMessage searchResEntry()*. Each *LDAPMessage searchResEntry()* is a result from the ldap server. This is essentially a row or record. So, if the query found 7 matches, then you should have 7 *LDAPMessage searchResEntry()* here. You can expand each *LDAPMessage searchResEntry()* to see the exact *objectName*, and the values.

Here you will see specifics of what the response from the ldap server. In particular, you can drill down to *protocolOp: searchRequest()*. Here you can see the *Filter* (this is the actual ldap query sent) that was used. You can also see the *attributes* that were requested. You can also see the *baseObject* here.

### SASL GSS-API Integrity: unbindRequest()

This is the disconnect from the ldap server. The clean up. The thing that tells the ldap server that we are done with it.



---

### \*\*\*Known issues with OpenLDAP/Active Directory

#### Ability to disable LDAP/Radius via the front panel

- resetpw (in the front panel “cmd” menu) disables LDAP/Radius (versions 5.3.0 and above)
  - Refer to Mantis case 3026
  - Available starting in version 5.3.0

Starting in version ~~5.2.1~~ (Apr 2015) 5.3.0 (Oct 2016) **resetpw also sets LDAP and Radius to “Disabled”** to help prevent total lockout. They need to be re-enabled thereafter, if desired. (Note- This change was inadvertently left out of the v5.2.1 release, so it was actually added in v5.3.0 (as verified by Keith).

When resetpw command is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled after performing a resetpw.

Q Help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?

**A Keith's response (23 May 17)** Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of 'admin123'.

Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn't change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.

---

### Known issues w/LDAP Groups with SSH

#### 1. (issue in versions 5.8.4/5.8.5) LDAP configuration for SSH

- Refer to Salesforce **Case 202731** and **JIRA Ticket SSS-671** (July 2019)
- Fixed in update version 5.8.6 (Oct 2019)
  - per 5.8.6 Release Notes: “Corrected problem with LDAP Groups used with SSH.”

Oz with Verizon reported to Dave Lorah on Case 202731: "I have a question on the LDAP configuration and ssh, is this supposed to work? Through t/s we noticed that ssh only works if we keep the local account on the server and then use our ldap password."

Hey Dave,  
We would configure the group section but we never see it get updated in nsswitch

```
spadmin@njbbsntp1 /etc $ cat nsswitch.conf
```

```
1. Begin /etc/nsswitch.conf
```

```
passwd: files ldap
group: files
shadow: files ldap
```

```
hosts: files dns
networks: files
```

```
protocols: files
services: files
ethers: files
rpc: files
```

as a result if we don't have a local account we see the following error.

```
Jul 10 20:34:51 njobbimsntp1 sshd[29725]: User pereos2 from 10.134.236.25 not allowed because not in any group
Jul 10 20:34:51 njobbimsntp1 sshd[29725]: Postponed keyboard-interactive for invalid user pereos2 from 10.134.236.25 port 49463 ssh2
[preauth]
Jul 10 20:34:55 njobbimsntp1 sshd[30016]: pam_ldap: error trying to bind as user "uid=pereos2,cn=users,cn=accounts,dc=nnodns,dc=com"
(Invalid credentials)
```

Dave L responded to Oz with:

Hi Oz,

We were able to reproduce the issue so no need to send us the log bundle. This may take some time to assemble a fix and test it. I believe this will be delivered in the form of a firmware patch so we will not need to wait for a firmware update release.

- I will let you know when we have the patch available.

## 2. (verison 5.4.5) Invalid configurations

### 3. (version 5.4.1) Apparent issue with LDAP connection to CLI (ssh). Web browser login with LDAP works fine

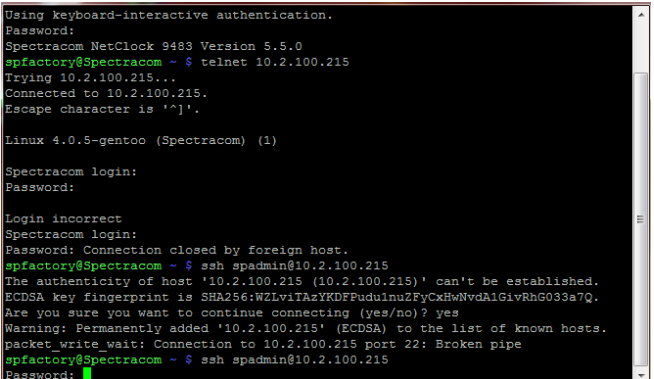
- V5.4.1 apparently has a connection timeout issue to SSH, even if LDAP is not enabled. With LDAP enabled, it can appear to be an issue with LDAP failing, but in reality its an issue with Ssh connection and not related to ldap.
- Due to the length of time it often takes to connect to ssh with 5.4.1 installed (even with LDAP disabled) the connection may timeout even before the login prompt is displayed. So it can appear as if there is an issue with LDAP connection to SSH,even though the browser login to an ldap account is just fine.

Disabling LDAP and trying to connect again with SSH results in the same affect with 5.4.1 (too long to connect). Once in a while, it will connect in about 10-15 seconds and if LDAP is enabled, login via ldap is successful. So LDAP with SSH in 5.4.1 is fine. When connecting via Linux box, this log timeout results in a “broken pipe message being reported.

Time to SSH connect with v5.5.0 installed, instead of 5.4.1, is just fine (with or without LDAP enabled).

See table below:

#### Time it takes to connect (before seeing the login prompt)

| Software Version | Telnet           | SSH (with or without LDAP enabled)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.5.0            | Almost instantly | About 4-6 seconds or sio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 5.4.1            | Almost instantly | <p><b>Often about 2 minutes</b> (periodically, it connects in about 10-15 seconds). When logging in with a linux box, this long login results in “<b>packet_write_wait:</b>” and then “<b>broken pipe</b>” being reported:</p>  <pre>Using keyboard-interactive authentication. Password: Spectracom NetClock 9483 Version 5.5.0 spfactory@Spectracom ~ \$ telnet 10.2.100.215 Trying 10.2.100.215... Connected to 10.2.100.215. Escape character is '^]'.  Linux 4.0.5-gentoo (Spectracom) (1)  Spectracom login: Password: Login incorrect Spectracom login: Password: Connection closed by foreign host. spfactory@Spectracom ~ \$ ssh spadmin@10.2.100.215 The authenticity of host '10.2.100.215 (10.2.100.215)' can't be established. ECDSA key fingerprint is SHA256:WZLviTAzYKDFPudulnuZFyCxHwNvdA1GivRhG033a7Q. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '10.2.100.215' (ECDSA) to the list of known hosts. packet write wait: Connection to 10.2.100.215 port 22: Broken pipe spfactory@Spectracom ~ \$ ssh spadmin@10.2.100.215 Password:</pre> |

---

**4. “Group filter” being enabled can cause very long delays in logging in (like 20 minutes for instance)**

Having the group filter enabled (“groups enabled”) can significantly increase the time it takes to authenticate/login (one customer reported it took 20 minutes to login). Disable this checkbox and see if the time it takes to login goes way down. If it does, the SecureSync having to search all of the groups is the reason for the long delay in logging in,

---

**5. (At least 5.4.1 and 5.4.5) Issue using the newer (black background) browser to enable LDAP to use SSL certificate**

- Refer to SR 6348 in SAP for an example.
- Not sure when this issue started, but its present in at least versions 5.4.1 and 5.4.5.
- Since its an issue with the black/charcoal browser only, can use the classic interface to configure the SSL certificate (note the Classic interface is disabled by default in 5.4.5- so it needs to first be enabled in order to use it). Refer to the LDAP/RadiusTech note for info on how to use the Classis interface to enable SSL with Radius

**Note:** the slider switch to enable the classic browser is in the **Management** -> **Network** page of the newer browser. Append 8080 to the end of the address to go into the classic browser.

---

**6. (After updating to 5.3.1) the SecureSync is constantly logging in and logging out of LDAP (several times a minute).**

- Refer to SR 4678 in SAP for details
- Noticed in 5.3.1, Expected to be fixed in 5.4.5

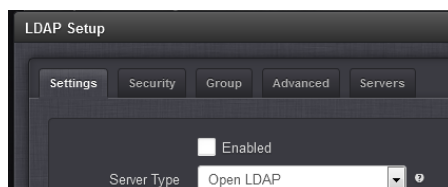
**Email from Paul Myers (30 Jun 16)** Hi Keith, We are including a new Key Type ED25519 in OpenSSH. I believe this is the issue why the customer was having errors reported in on login because it was looking for this keytype.

If this is NOT the ldap related login issue, we are NOT fixing it for the next release as other than finding we didn't correctly support the new key type we have nothing else to go on.

---

**7. (Version 5.3.1: Applies only to “OpenLDAP” configuration - not to “active directory”) NSS password is a required field though its not needed for OpenLDAP and the field isn’t displayed to even be able to enter a value:**

- Refer to Mantis case 3233/Salesforce case 21297.
- Fix should be in version 5.4.0 update (~March 2016)
- Occus only when “OpenLDAP” is selected in the “Server Type” field (This isn’t an issue when “Active Directory” is selected):



---

**8. (prior to 5.2.0) Issues with group authentication (should be fixed in 5.2.0 and above)**

- Refer to “Group Authentication” sub-section further above for details.

---

**9. (prior to 5.1.7) Fields are Greyed-out**

- Update to at least v5.1.7 to be able to login using LDAP and have admin rights unless an account was created on the time server.
- Earlier versions wouldn't allow access with admin rights.

---

**10. (5.1.5 and below) require an account be created on the box**

- If the unit is shipped with version 5.1.5 installed (or is updated in the field to v5.1.5 and then cleaned) LDAP will fail unless a user account is created which has the same username as the box. The password used to create the account should be different than the one in the LDAP server.

---

**11. (4.8.1 and below) "Not Supported" displayed**

- With Archive Versions 4.8.1 and below installed, a minor bug causes "Not Supported" to be displayed in the LCD, even though the command did reset the password.

## \*\*\*Troubleshooting LDAP

### CLI command to list all users

**Per Ron Dries (21 April 2020)** For a command line way to list users, including LDAP users, issue the following command: `getent passwd<enter>`

**Note:** The ldap.conf file is located in `/etc/ldap.conf`

- 1) If software version is at least 5.1.6 or below, a user account needs to be created in the SecureSync (or update to a newer version of software which fixes this issue). Refer to the list of known LDAP issues above for more info.
- 2) cat the ldap.conf file (`/etc/ldap.conf`) (spadmin account can view all of this file)

```
spadmin@SpectraCom ~ $ cd /etc
spadmin@SpectraCom /etc $ cat ldap.conf
version 3
scope sub
timelimit 120
bind_timelimit 120
uri ldap://orodc02.int.oro.ia.com/
base dc=int,dc=oro.ia,dc=com
binddn CN=ldaptest,OU=ROC-IT,OU=ROC,DC=int,DC=oro.ia,DC=com
bindpw Password12
tls_checkpeer no
# ad
pam_filter objectclass=user
pam_login_attribute sAMAccountName
nss_base_passwd OU=ROC-IT,OU=ROC,?sub
nss_base_shadow OU=ROC-IT,OU=ROC,?sub
nss_map_objectclass posixAccount User
nss_map_objectclass shadowAccount User
nss_map_attribute uid sAMAccountName
nss_map_attribute cn sAMAccountName
nss_map_attribute uniqueMember member
nss_override_attribute_value unixHomeDirectory /home/spectra.com
nss_override_attribute_value LoginShell /bin/bash
```

- 3) Is LDAP login to classic interface browser successful? If it is, the LDAP Server settings are valid.
- 4) Is LDAP login to both the web browser and CLI failing? Or, is ldap login to just the browser, or to just the CLI working fine, while failing on the other interface?
- 5) Get at least the full **Auth log, System log, User log and Journal log** (or just get a full log bundle)
- 6) Review the **Auth, USER and System** log (especially the User logs which logs errors)
- 7) Delete and re-enter the Radius server(s) using an intentionally wrong shared secret key and grab the logs. See if the System log contains the following entry **pam\_radius\_auth: packet from RADIUS server 10.82.122.16 fails verification: The shared secret is probably incorrect.** This entry indicates the SecureSync is communicating with the Radius server.
- 8) Re-enter the Radius server using the correct Shared secret key and try logging in.
- 9) Make sure LDAP port 389 (and 636 for SSL) is open on firewalls between the SecureSync and Radius server:
- 10) Make sure the main default port/gateway is configured properly so that the SecureSync can route to the LDAP server.

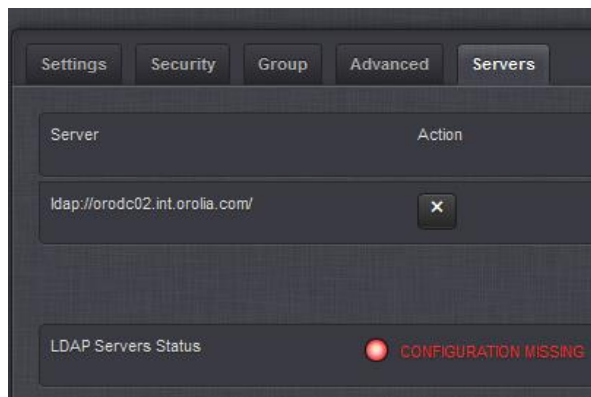
**Partial email from Keith (20 Oct 16)** Is the configured LDAP server on the same subnet as the SecureSync' Ethernet interface(s)? If its not on the same subnet as the base Ethernet port "eth0" (or one of the three additional Ethernet interfaces, if the Model 1204-06 Gb Ethernet Option Card is installed), please ,make sure the correct main default port/gateway is configured correctly so that the SecureSync knows how to be routed to the LDAP server (as configured in the **Management -> Network Setup** page of the web browser. On the left side of this page, press the **General Settings** button and select the correct **Default Port** drop-down).

- 11) Make sure DNS is setup correctly if using hostname of the LDAP server (try temporarily using an IP address instead of the hostname. If it connects, issue is related to DNS).

**Partial email from Keith (20 Oct 16)** Is the LDAP server specified in the **Management -> Authentication -> LDAP Setup** page of the browser (Servers tab) using its IP address or its DNS name? If its configured using its DNS name, try at least temporarily changing its name to its IP address and then try logging in again to the LDAP server. If it now allows the SecureSync to connect to the LDAP server, the issue is associated with DNS identifying the LDAP server.

5735764276

- 12) **“NSS password” field left blank:** login will take a long time but will still result in a successful login.
- 13) **“LDAP Servers Status” (Servers tab )** always reports **“configuration missing”** in at least versions 5.1.5 and below (as shown below)



**LDAP with web browser works fine. BUT LDAP with CLI/SSH not working (associated with any software version being installed)**

### Defining the LDAP/Radius account login permissions (user or admin)

Unlike earlier NetClocks, the SecureSyncs and 9400s don't need a user account created in the box. So there is no longer a place to configure whether the account has admin or user rights in the NTP server itself. For these units, this needs to be configured in the LDAP or Radius server.

### LDAP account permissions

For **LDAP**, refer to: **“Specific LDAP Server Configuration”** in the LDAP section of the Radius/LDAP Tech note in the SecureSync folder (pasted below, as well)

### Specific LDAP Server Configuration

Follow the instructions specific to your LDAP server(s) to create and modify users in the LDAP server(s).

A SecureSync LDAP user needs the following LDAP fields:

|                  |                                                                                      |
|------------------|--------------------------------------------------------------------------------------|
| homeDirectory    | /home/spectracom                                                                     |
| loginShell       | /bin/bash                                                                            |
| uid              | A user name, (not “spadmin”)                                                         |
| uidNumber        | Use a number outside the range 1000 to 1050                                          |
| <b>gidNumber</b> | <b>“admin”</b> group is “111”, <b>“user”</b> group is “112” (See <b>Notes</b> below) |
| userPassword     | <password>                                                                           |

## **gidNumber attribute (used for SecureSync's CLI interface only- not used for web browser access)**

**Note:** "gidNumber" defines the permissions for each account, to be either **admin** account or **user** account. But only the **CLI interface** cares about this value. The web browser doesn't care, so LDAP users will be able to still use the browser, whether or not this attribute is assigned. But the CLI interface will not be accessible if this value is not assigned.

**Note:** The gidNumber is only used for access to **SecureSync's CLI interface** (such as telnet/SSH sessions). If the GID is not assigned as either of these two values, LDAP users won't be able to access CLI connections, but they **will still be able to access/use the web browser**, with admin rights. If scripting is desired to be used, the available REST API interface can be used, in lieu of logging into the SecureSync's dedicated CLI interface.

### **(Case 186110): customer doesn't want to assign gidNumber 111 or 112 to all his AD accounts**

**email from Ron Dries, after checking with Stuart (20 Feb 2019)** The web UI should allow them to login without the gid set. All of the status and configuration they need can be done through the UI. If they need to script things they can use the REST API.

**Keiths response to this customer (20 Feb 2019) based on the response above from Ron** Note for your reference, I had assigned our Support case number 186110 to your questions. I apologize for the delay in being able to respond back to you, as I needed to first clarify a couple points with our Engineering team.

With some input from our Engineers, attached you should find a slightly revised copy of the SecureSync LDAP/Radius tech note you had mentioned referring to. I have updated the gidNumber info on page 14 of this document.

Specific to your questions/concerns of needing to hard-assign one of the two gidNumber attributes to your AD accounts, I found out that not performing this task results in only one very minor limitation (the CLI interface won't be accessible to the AD users).

The gidNumber attribute only applies to the SecureSync's CLI interface (such as telnet/ssh/ftp/scp connections). The CLI interface needs this attribute to be defined correctly, in order for the users' permissions to be provided by the AD server (unlike "local" accounts, such as the spadmin account, which have these permissions defined/stored inside the SecureSync itself).

However, the SecureSync's web browser doesn't utilize the gidNumber attribute. If an LDAP user has been authorized by AD to access the SecureSync, that user will automatically have permission to access/use the browser interface. It doesn't matter to the browser if this attribute is set to 111,112, or any other value.

As the browser provides the ability to perform all configurations of the SecureSync, not defining the gidNumber (thereby, only preventing access to the CLI interface, but not the browser) provides no configuration limitations. And if by chance its desired for AD accounts to be able to perform scripting, the available REST API (having the same permissions as the web browser) can be used to perform this task, in lieu of having access to the dedicated CLI interface.

Please let us know if you would like additional information pertaining to the availability of the REST API interface for the browser.

### **Active directory permissions (user or admin)**

**Q.** The instructions to setup different permissions levels, that is shown below, doesn't make sense to me. I can not setup a "gidNumber" with my active directory. Maybe these instructions are more Linux based machines? How do I do this is active directory? I will attach a screenshot of all the attributes of a user on my active directory.

**A Email from Dave Sohn (19 Mar 2013)** "Below is my best effort. I can't guarantee all of this, but I believe this is all accurate."

I believe the information that is requested for the Specific LDAP Server Configuration is independent of Linux or Windows. This needs to be present on both. If the user completes authentication, but an object like the Group ID is missing, then they will default to user privileges. I don't have a Windows Server 2008 installation to look at, but on the Windows Server 2003 I can see these. They need to enable editing/display of UNIX attributes, which means the schema of their Active Directory installation needs to be extended. They should have installed "Identity

Management for UNIX” role service installed. You should now see a tab labeled “UNIX Attributes” in the properties for users and groups. The group ID of the domain group used to collect users for the SecureSync management needs to be set to **111 or 112** depending on admin or user privileges. Then for each of the users, you need to setup their UNIX attributes as described and make them a member of that group within the UNIX attributes

---

NTPSERVER sudo: nss\_ldap: failed to bind to LDAP server ldap://10.0.100.30: Invalid credentials

NTPSERVER sudo: nss\_ldap: could not search LDAP server - Server is unavailable

- (Note: not sure if these entries were from the Auth log or the User log)

**Appears to be associated with the LDAP Bind password for connecting with the LDAP sever (not the ldap login itself)**

- Make sure the account being used has sufficient permissions to be able to “search the datababse”
- This particular customer (who saw the error message above) was initially using special characters in their Bind DN and/or Bind password. Worked fine after removing the special characters:
  - “I changed the password for the BIND and that fixed the problem. Apparently it didn't like one of the special characters. I was using a password with **&#(\$** in it”

---

## Auth log entries

**apache2: pam\_security(login:account: cannot determine user's tty**

**Cause:** the LDAP server is looking in the SecureSync for the user account but can't find it. This will happen. This is a known issue with software versions 5.1.3 and 5.1.4 that require a user account be created on the SecureSync. Refer to known issues further below.

---

## User log entries

- **Note:** Valid LDAP logins do not result in any User (or Auth) log entries.
- **Note:** to see the latest entry of the user log in CLI connection: **tail -f log/user.log**

**apache2: pam\_ldap: missing “host” in file “/etc/ldap.con**

**Cause:** “Servers” tab of the **Management** -> **LDAP** page of the browser does not have any LDAP servers listed.

**apache2: pam\_ldap: ldap\_initialize Bad parameter to an ldap routine**

**Cause:** Can't find the LDAP server on the network

### Possible reasons

- **IP address-** when using the LDAP server's IP address, the IP address MUST be in URI format (the configured IP address must begin with the following: **ldap://** (example: **ldap://xxx.xxx.xxx.xxx**)
- **DNS hostname:** when using the LDAP server's hostname , the hostname MUST be in URI format (the configured hostname must begin with the following: **ldap://** (example: **ldap://icrosoft.com**)
- **Configured LDAP server isn't an LDAP server** (SecureSync can reach it, but it's not an LDAP server).



**Note:** I saw this here by adding a second LDAP server using the IP address of one of our SecureSyncs (10.2.100.176). LDAP login was not successful, even though other server was fine (Deleted this second “server” and logged in successfully)

- “Servers” tab of the **Management** -> **LDAP** page of the browser does not have a valid or LDAP Server address configured.
- If a hostname is listed instead of an address, could be DNS is not configured correctly in the **Management** -> **Network** page of the browser, (Gear box ICON the particular network interface). Try temporarily using its IP address.
- LDAP server requires SSL connection, but the LDAP Server’s certificates/keys aren’t loaded.

**Email from Keith (8 Sept 2014)** Does your LDAP server require an encrypted SSL connection? If it does, make sure port 636 is also open on any firewalls and go to the **Management** -> **Authentication** page of the browser, **LDAP Setup** button (where the LDAP settings are). Make sure the server and client certificates and Client key for your LDAP server are properly installed (click on the “i” ICON next to each of these settings to verify whether or not they are currently installed, as may be required by your LDAP server. If it’s required, and these aren’t loaded or are invalid, the SecureSync won’t be able to communicate with the LDAP server.

- **Main default gateway issue.**

|                                        |              |
|----------------------------------------|--------------|
| Domain                                 | domain201    |
| DNS Primary                            | 10.1.1.20    |
| DNS Secondary                          | 10.1.1.31    |
| <input type="checkbox"/> Enable DHCPv4 |              |
| Static IPv4 Address                    | 10.2.100.176 |
| Netmask                                | 255.255.0.0  |

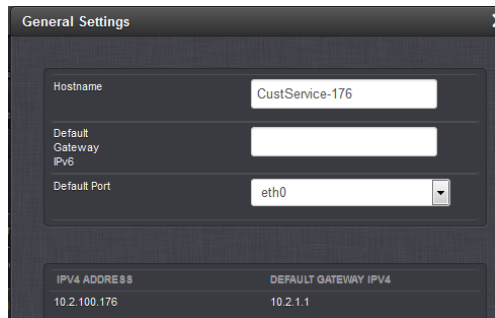
**Email from Keith (8 Sept 2014)** Go to the **Management** -> **Authentication** page of the browser, **LDAP Setup** button (where the LDAP settings are). Then click on the **Servers** tab at the top. As shown below, the LDAP server’s IP address or hostname should be listed.

Is the Server’s IP address or its hostname listed in this pop-up window? Either way, make sure this value is correct for that server. If it’s the hostname one suggestion is temporarily enter a “new server” using its IP address instead of its hostname and fill in the rest of the configuration for that server. Logout and login using the correct credentials.

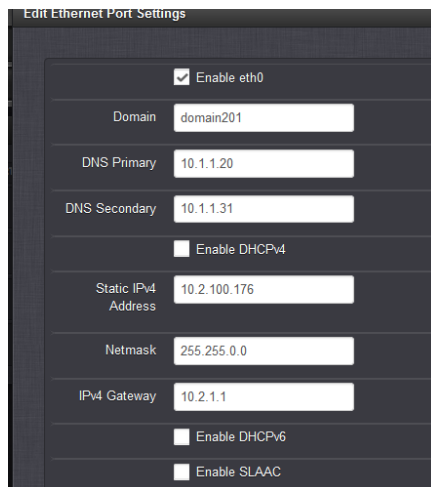
If login was successful, the issue is related to DNS configuration. Go to the **Management** -> **Network** page of the browser. Click on the gear box for the Ethernet port that goes to the LDAP server. Verify the domain and DNS server(s) are entered correctly for the network. Also verify the main default port/gateway address is configured correctly (**Management** -> **General Settings**) page of the browser.

### apache2: pam\_ldap: ldap\_simple\_bind Can’t contact LDAP server

- Cause: can’t reach the LDAP server on the network
- I saw it here when there was an error in the default gateway address for Eth0. So it wasn’t able to reach the LDAP server. Management -> General Setup page of the browser a



- DNS- Also saw it here when the DNS sever values were deleted. DNS has to be setup correctly if using the DNS hostname for the LDAP server (instead of configuring its IP address). DNS is configured in the Management -> Network page of the browser and edit the particular port that goes to the DNS server.



### apache2: could not search LDAP server - Server is unavailable

**Cause:** issue with LDAP server or with its associated network

### apache2: pam\_ldap: error trying to bind as user "CN=ldaptest,OU=ROC-IT Users,OU=ROC-IT,OU=ROC,DC=int,DC=orolia,DC=com" (Invalid credentials)

**Causes** (*Management* -> *Authentication* -> page of the browser, **LDAP Setup** button)

- Valid account name, but invalid password OR
- invalid account name

### apache2: pam\_ldap: ldap\_search\_s Referral

**Cause:** invalid "Search Base DN" field (*Management* -> *Authentication* -> page of the browser, **LDAP Setup** button)

### apache2: pam\_ldap: ldap\_search\_s No such object

### apache2: pam\_ldap: ldap\_search\_s Invalid DN syntax

**Cause** (Note there may be more than one reason)

- I saw it here and couldn't login when there was an error in the **NSS password** field (I cleared this field

and resolved this entry).

## apache2: pam\_ldap: error trying to bind (Invalid credentials)

### possible causes:

- invalid “**Bind DN**” field OR
- invalid “**Bind password**” field
- invalid “**NSS password**” field (note that successful LDAP login can still occur if this field is left null or possibly if it's incorrect, but this log entry is asserted if the correct value is not entered).

## apache2: pam\_ldap: ldap\_search\_s Operations error

### Cause (Note there may be more than one reason)

I saw it here when there was a missing comma in the **NSS password** field (*Management* -> *Authentication* -> page of the browser, **LDAP Setup** button).

---

## Known issues with LDAP

### 1) LDAP Groups with SSH (applicable to versions 5.8.4 and 5.8.5)

#### (issue in versions 5.8.4/5.8.5) LDAP configuration for SSH

- Refer to Salesforce **Case 202731** and **JIRA Ticket SSS-671** (July 2019)
- Fixed in update version 5.8.6 (Oct 2019)
  - per 5.8.6 Release Notes: “Corrected problem with LDAP Groups used with SSH.”

**Oz with Verizon reported to Dave Lorah on Case 202731:** "I have a question on the LDAP configuration and ssh, is this supposed to work? Through t/s we noticed that ssh only works if we keep the local account on the server and then use our ldap password."

Hey Dave,  
We would configure the group section but we never see it get updated in nsswitch

```
spadmin@njbbsntp1 /etc $ cat nsswitch.conf
```

```
2. Begin /etc/nsswitch.conf
```

```
passwd: files ldap  
group: files  
shadow: files ldap
```

```
hosts: files dns  
networks: files
```

```
protocols: files  
services: files  
ethers: files  
rpc: files
```

as a result if we don't have a local account we see the following error.

```
Jul 10 20:34:51 njbbmsntp1 sshd[29725]: User pereos2 from 10.134.236.25 not allowed because not in any group  
Jul 10 20:34:51 njbbmsntp1 sshd[29725]: Postponed keyboard-interactive for invalid user pereos2 from 10.134.236.25 port 49463 ssh2 [preauth]  
Jul 10 20:34:55 njbbmsntp1 sshd[30016]: pam_ldap: error trying to bind as user "uid=pereos2,cn=users,cn=accounts,dc=nnodns,dc=com" (Invalid credentials)
```

**Dave L responded to Oz with:**

Hi Oz,

We were able to reproduce the issue, so no need to send us the log bundle. This may take some time to assemble a fix and

test it. I believe this will be delivered in the form of a firmware patch so we will not need to wait for a firmware update release.

---

## 2) LDAP Security (SSL certificate required by LDAP server) in software versions 5.4.5 and below

- LDAP Setup page, Security tab (newer browser) for SSL certificate doesn't work correctly in v5.4.5 and below.
  - Need to either use the classic interface browser in versions 5.4.5 and below to configure SSL (instead of using newer browser) , or update the software to at least v5.5.0.
- 

## 3) LDAP in software versions 5.1.4 and 5.1.5

- Mantis case 2894 (Same as Mantis case 2832 below in version 5.1.4)

### Details:

- If the unit was purchased with versions 5.1.4 or 5.1.5 installed a user account needs to be temporarily added.
  - If the unit was updated to versions 5.1.4 or 5.1.5 and then cleaned: a user account needs to be temporarily added.
  - If the unit was updated to versions 5.1.4 or 5.1.5 and hasn't been cleaned, no account is needed
- Mantis case 2834: LDAP Servers status (Servers tab) reports "Configuration missing" even though LDAP is working just fine.
  - Mantis case 2832: Per Ron Dries- Not sure exactly why, but if the time server is clean updated from 5.1.3 to 5.1.4 (or purchased with 5.1.4, a user account needs to be created in the SecureSync in order to use this function. However, if it's updated from 5.1.3 to 5.1.4 without performing a clean, a user account does not need to be created.

If an account needs to be created -The username has to be the same as the LDAP username, but the account password does not need to be the same as the LDAP password for it to work. Suspect this will be fixed in 5.1.6.

## 4) LDAP in Archive software version 5.1.2

- Mantis case 2432: LDAP server add is broken

Due to a file pointer issue in 5.1.2, Radius in the new web browser doesn't allow a user to be able to login. With the "Classic interface" web browser, if a user successfully authenticates with the Radius server, they are logged in, but only with user-rights (fields are grayed-out).

## 5) LDAP in Archive software versions 5.0.1 and 5.0.2 not working

- Mantis case 2419: can login for a couple of hours and then stops

## 6) LDAP and Radius in version 5.0.2

- Mantis case 2450: remote users can't login.

---

## TACACS + (Remote authentication)

TACACS info (in online SecureSync user guide):

### Summary

- Refer to online 1200 SecureSync user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/TACACS.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm)
- “TACACS +” was added as part of update version 5.5.0 (~Dec, 2016, reference ECO 1080)
  - Tacacs/Tacacs + is not available in versions prior to 5.5.0

### What is TACACS

- Refer also to RFC 1492: <https://tools.ietf.org/html/rfc1492>

(From Wikipedia) **Terminal Access Controller Access-Control System (TACACS)** is a remote [authentication protocol](#) that is used to communicate with an authentication server commonly used in [UNIX](#) networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network. TACACS is defined in [RFC 1492](#), and uses (either [TCP](#) or [UDP](#)) port 49 by default.

attribute

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back. The TIP (routing node accepting dial-up line connections, which the user would normally want to log in into) would then allow access or not, based upon the response. In this way, the process of making the decision is "opened up" and the algorithms and data used to make the decision are under the complete control of whomever is running the TACACS daemon.

A later version of TACACS introduced by Cisco in 1990 was called **Extended TACACS (XTACACS)**. The XTACACS protocol was developed by and is proprietary to [Cisco Systems](#).

**Terminal Access Controller Access-Control System Plus (TACACS+)** is a protocol developed by Cisco and released as an open standard beginning in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles [authentication, authorization, and accounting \(AAA\)](#) services. TACACS+ and other flexible AAA protocols have largely replaced their predecessors.

[TACACS+](#) and [RADIUS](#) have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Since TCP is connection oriented protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet lost, timeout etc. since it rides on [UDP](#) which is connectionless.

RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks.

TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.

---

## Tacacs AAA (Authentication, Authorization, Accounting)

- TACACS can do much more (Authentication, Authorization, Accounting) than what the SecureSync supports
- SecureSync only supports Tacacs for **Authenticaton** (it doesn't support **Authorization** or **Accounting**)

(Below Is from: <https://www.networkworld.com/article/2838882/radius-versus-tacacs.html>)

**Before allowing and entity to perform certain actions, you must:**

- Ensure you know who that entity actually is (**Authentication**) (Supported in SecureSync)
- And if the entity is authorized to perform that action (**Authorization**).
- Additionally, you need to ensure that accurate records are maintained showing that the action has

occurred, so you keep a security log of the events (**Accounting**).

---

## Cisco ISE (Identity Services Engine)

### What is ISE TACACS+ Server



Cisco ISE is a **security policy management platform that provides secure access to network resources**. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations.

### Cisco ISE apparently not supported in 1200 SecureSyncs

- Refer to Salesforce Cases such as **283987** (and JIRA ticket **DMND-1842**, submitted 12 Aug 2022, for Model 2400 SecureSyncs)
- Appears to be due to SecureSyncs not supporting TACACS Authorization functionality (not sure whether TACACS Accounting functionality is also required by ISE)

---

### TACACS+ User rights/permissions/privileges/role based authentication (admin/user)

- Refer to Salesforce Cases such as 251723 (Nov 2020)
  - **Per Chris Olin (20 Nov 2020)** I was able to speak with one of our engineering directors about this today who confirmed it is a planned feature, but is not currently targeted for a future release.

**Per Ron Dries (19 May 2020, as of at least v5.8.9 and below)** Currently TACACS+ users always have **admin** privileges when logged into SecureSync.

**Per Dave Sohn (22 May 2020, as of at least v5.8.9 and below)** We do not have currently support role based authentication controls via TACACS+. The only centralized service we currently support with that capability is LDAP. Additionally, we do not have read-only user roles available within SecureSync, just admin and user levels.

---

### TACACS users can login to the browser or CLI interface

**Per Ron Dries (19 May 2020, as of at least v5.8.9 and below)** TACACS+ users can login via the CLI and GUI.

---

## TACACS security

### What method is the SecureSync using for TACACS auth protocol (PAP, CHAP, EAP)?

- Tacacs+ uses TCP port 49

Q One follow up question: what method is the SecureSync using for TACACS auth protocol? PAP, CHAP, EAP?

**A Reply from Pritam (16 June 2020)** TACACS uses TCP protocol so it will not use any PAP, CHAP or EAP type authentication method. In fact TACACS demon will encrypt entire communication between the Server and the client/NAS hence do not require authentication method.. If more details is needed it can be found in RFC 1492.

And I do not know why our manual is asking either PAP or Global methods. One thing I can think of is – TACACS+ has compatibility for PAP method when the P2P protocols (Not Ethernet - like SDH, ATM, Frame Relay) are in use.

## Packet Encryption

Info below from [https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp\\_udp\\_tcp](https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp_udp_tcp)

*RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.*

*TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.*

---

## SecureSync software version-related info for TACACS

### Version 5.8.9

- Per the 5.8.9 Release Notes: Repaired TACACS+ username functionality to allow the “\_” character

### Version 5.8.3 (Jan 2019)

- Per the 5.8.3 Release Notes “Fixed an issue in which clean updates wouldn’t allow TACACS+ access through http”

### After performing an upgrade to version 5.8.2 (or above) from a previous version 5.8.0 or 5.8.1

- After updating to 5.8.2 (or above) from either versions 5.8.0 or 5.8.1 **SSH with TACACS may work fine**, while **browser with TACACS login** doesn’t work. This is due to two lines in a config file being reversed during the earlier to newer software update proces (not actually an issue in 5.8.2 or above) if a restore to defaults update is performed from versios 5.8.0 or 5.8.1
- The simple fix is to toggle TACACS off and back on (ensure the Submit button is pressed after unchecking the “HTTP/HTTPS” checkbox and then presssubmit a second time after re-selecting the checkbox). the order of the two lines is corrected when TACACS is disabled and then re-enabled.
- Refer to TACACS troubleshooting further below for more details

### (Starting with software update version v5.6.0 (and above))

- TACACS now works with both the browser and the CLI interface (ssh, ftp etc)
- Software version 5.6.0 (Apr 17) added login user authentication support for protocols other than HTTP/HTTPS (web browser). Now supports CLI interface as well (such as ssh, telnet and FTP/SCP)

## Starting with software update version 5.5.0 (and above)

- “TACACS +” is now supported (as an alternate to using Radius)
- Note that until version 5.6.0, TACACS only works with the web browser (not the cli interface)

---

## Configuration of the Tacacs server itself/Message types

*From:* <https://www.networkworld.com/article/2838882/radius-versus-tacacs.html>

TACACS+ communication between the client and server uses different message types depending on the function. In other words, different messages may be used for authentication than are used for authorization and accounting. Another very interesting point to know is that TACACS+ communication will encrypt the entire packet.

## Tacacs Authentication messages (we only support Authentication messages:

- Refer to sites such as: <https://tools.ietf.org/id/draft-ietf-opsawg-tacacs-07.html>
- Refer also to **RFC 1492**: <https://tools.ietf.org/html/rfc1492>
  - The Authentication **START** Packet Body
  - The Authentication **REPLY** Packet Body
  - The Authentication **CONTINUE** Packet Body

## Description of Authentication Process

The action, `authen_type` and `authen_service` fields (described above) combine to determine what kind of authentication is to be performed. Every authentication **START**, **REPLY** and **CONTINUE** packet includes a data field. The use of this field is dependent upon the kind of the Authentication.

A set of standard kinds of authentication is defined in this document. Each authentication flow consists of a **START** packet. The server responds either with a request for more information (**GETDATA**, **GETUSER** or **GETPASS**) or a termination (**PASS** or **FAIL**). The actions and meanings when the server sends a **RESTART**, **ERROR** or **FOLLOW** are common and are described further below.

When the **REPLY** status equals `TAC_PLUS_AUTHEN_STATUS_GETDATA`, `TAC_PLUS_AUTHEN_STATUS_GETUSER` or `TAC_PLUS_AUTHEN_STATUS_GETPASS`, then authentication continues and the **SHOULD** provide `server_msg` content for the client to prompt the user for more information. The client **MUST** then return a **CONTINUE** packet containing the requested information in the `user_msg` field.

All three cause the same action to be performed, but the use of `TAC_PLUS_AUTHEN_STATUS_GETUSER`, indicates to the client that the user response will be interpreted as a username, and for `TAC_PLUS_AUTHEN_STATUS_GETPASS`, that the user response represents will be interpreted as a password. `TAC_PLUS_AUTHEN_STATUS_GETDATA` is the generic request for more information to flexibly support future requirements. If the `TAC_PLUS_REPLY_FLAG_NOECHO` flag is set in the **REPLY**, then the user response must not be echoed as it is entered. The data field is only used in the **REPLY** where explicitly defined below.



---

## Configuration of TACACS + in 1200 SecureSyncs / TACACS config files

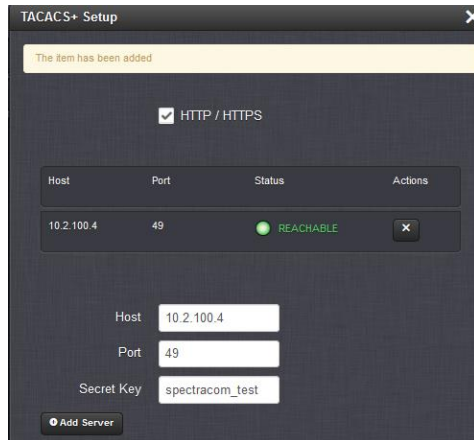
### A) Our Tacacs server settings for testing Tacacs (note this info may have since changed)

Server: 10.10.241.249

Port: 49

secret key: [spectracom\\_test](#) (all lower-case)

*after pressing “add Server”*



**Test account to login as (this account shouldn't be added to the SecureSync)**

User name: [testuser](#)

password: [testpwd](#) (all lower-case)

**Journal log after adding the above (v5.8.2)**

**“[Saved Tacacs Server data \(spadmin\)](#)”**

---

### B) Configuration of fielded 1200 SecureSyncs

- Refer to online SecureSync user guide at:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/TACACS.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm)
- Refer to Cisco's “TACACS+ Configuration Guide” ( [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-usr-tacacs-att-value-pairs.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-usr-tacacs-att-value-pairs.html))
- SecureSync only uses the Tacacs account for Authentication. (The SecureSync doesn't support AAA - [authentication](#), [authorization](#), [accounting](#))
- Tacacs server should work with just fine with a generic TACACS config

Q (From Case 236694) “I'd like to get additional details on setting up TACACS+ on the SecureSync. The instructions provide no details beyond how to add the TACACS+ server, **but I need to know what kind of TACACS+ response the SecureSync expects.** For example, what kind of response should I send for authorization. I tried using LDAP and RADIUS, but the LDAP requirements for having homeDirectory, loginShell, etc for the user's won't work for us. And RADIUS only supporting PAP isn't secure enough for us to use. So any guidance on TACACS+ would be greatly appreciated.

**A Reply from Pritam (16 June 2020)** “They would need to create a user account in their TACACS server that can be authenticated. Our SecureSync only uses the TACACS account for Authentication.”

**A Reply from Keith to customer (16 June 2030)**

### **My response**

In summary, the only configuration necessary to use the Tacacs Authentication functionality supported by the SecureSync, is to:

- 1) Configure the Tacacs server info in the SecureSync (as you alluded to, and as discussed in the online SecureSync user guide at:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/TACACS.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm)
- 2) Have one or more accounts created on the Tacacs server, which support authentication (can be authenticated). Just make sure the account names (and any derivatives of the account names) created on the Tacacs server and desired to be used with the SecureSync, are not also in the SecureSync itself (these include the default account name of "spadmin", and any other accounts which can optionally be created in the SecureSync for local login).

There should be no "manual configuration" necessary of the response sent to the SecureSync. The Tacacs should send an authentication message when the account credentials are authenticated (the SecureSync only supports the Authentication functionality of the Tacacs protocol).

When a user tries logging into the SecureSync's browser or CLI interface using a Tacacs account (not using "spadmin" or any optional local accounts which may have been created in the SecureSync), the Tacacs server verifies the login credentials entered and then lets the SecureSync know that the user can be logged in as an admin user.

Please let me know you can successfully login to the SecureSync's browser and CLI interface as an admin user, when using valid Tacacs account credentials, after configuring the Tacacs server info in the SecureSync. Thanks in advance.

---

### **Adding/Removing a TACACS server**

- Refer to online SecureSync user guide at:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/TACACS.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm)

**Management -> Authentication -> "TACACS+ Setup" button**

### **Journal log asserted after adding a TACACS server (v5.8.2)**

**"Saved Tacacs Server data (spadmin)"**

---

### **Tacacs Attribute info/Attribute-Value (AV) Pairs**

- Refer to sites such as: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-usr-tacacs-att-value-pairs.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-usr-tacacs-att-value-pairs.html) (excerpt below):  
*Terminal Access Controller Access Control System Plus (TACACS+) attribute-value (AV) pairs are used to define specific authentication, authorization, and accounting elements in a user profile that is stored on the TACACS+ daemon.*
- In part, used to assign either Admin or User rights/permissions
- Not supported (as of at least versions 1.6.0 and below. We only support Authentication- we don't support Authorization and Accounting)
  - Refer to JIRA ticket **DMND-1842**, submitted 12 Aug 2022, for Model 2400 SecureSyncs)

Q I'm in the process of enabling Tacacs+ on our NTP/PTP appliances and the below question is being asked by our Clearpass engineer... If you can get any TACACS+ attribute info from the vendor (ppp:ip AV-pairs) that would be helpful.

**A Per Pritam (31 July 2020) It is correct we only support Authentication part of TACACS+. Authorization and Accounting piece is not supported.**

A Reply from Dave L to customer (31 July 2020) We do not support the TACACS+ Attribute Value pairs feature in the Securesync or Velasync products.

## TACACS+ User rights/permissions/privileges/role based authentication (admin/user)

Refer to Salesforce Cases such as 251723 (Nov 2020)

**Per Chris Olin (20 Nov 2020)** I was able to speak with one of our engineering directors about this today who confirmed it is a planned feature, but is not currently targeted for a future release.

**Per Ron Dries (19 May 2020, as of at least v5.8.9 and below)** Currently TACACS+ users always have **admin** privileges when logged into SecureSync.

**Per Dave Sohn (22 May 2020, as of at least v5.8.9 and below)** We do not have currently support role based authentication controls via TACACS+. The only centralized service we currently support with that capability is LDAP. Additionally, we do not have read-only user roles available within SecureSync, just admin and user levels.

---

## TACACS config files

- both `/etc/tacacs.conf` and `etc/tacacs_pam.conf` appear to be identical

### A) `tacacs.conf` file is located in `/etc` folder

*Example tacacs.conf file from one of our 5.8.0 units with TACACS login functional*

```
too many parameters.
spfactory@Spectracom /etc $ cat tacacs.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user_notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.100.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip server=10.2.100.4:49 secret=spectracom_test
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip server=10.2.100.4:49 secret=spectracom_test
spfactory@Spectracom /etc $ █
```

### B) `tacacs_pam.conf` config file)

- Path to `tacacs_pam.conf` file `/etc/` and then type `cat tacacs_pam.conf`

*Example tacacs\_pam.conf file from one of our units with TACACS login functional*

```
spfactory@Spectracom /etc $ cat tacacs_pam.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user_notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.10
0.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
spfactory@Spectracom /etc $ █
```

TACACS account cannot also be a user account created in the unit

**Caution:** In order to utilize TACACS+ authentication, the account username on the TACACS+ server must NOT be used with a local user account.

**EXAMPLE:** Can't create a username such as "username" in both the TACACS server and in the SecureSync. Create the user account on the TACACS server only (not in the SecureSync also).

- If the TACACS account name has been added as a useraccount in the SecureSync, trying to login with the TACACS account name will respond with "Access Denied". Delete the user in the SecureSync via the **Management** -> **Authorization** page of the browser
- Refer to online SecureSync guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/TACACS.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm)

### Notes about user account names/.addlocal temporary account

- 1) The user account name can only be in the TACACS server (the same username cant be in the SecureSync also)
- 2) (applicable to versions 5.8.8 and below) the TACACS username cannot contain an underscore ("\_"). Per the 5.8.9 Release Notes: [Repaired TACACS+ username functionality to allow the "\\_" character](#)
- 3) The username cannot be the same as any of the account names created by factory default (such as spadmin, spfactory, spui, etc)
- 4) each time a TACACS account name is used with a successful CLI login (such as ssh – not with the browser, this account name is temporarily added/stored in a file named addlocal (located in **/etc**). Viewing the contents of "addlocal" will show the custom account names that which been used to login via the CLI interface (to view the contents in ssh, cd to **/etc**, type: **cat addlocal**)

```
testusr!!:17639:0:99999:7:::
spfactory@Spectracom /etc $ cat addlocal
sspadmin 1524075083
testusr 1524055047
spfactory@Spectracom /etc $
```

**Note:** the username(s) is cleared from the addlocal table upon reboot or when performing a "logout" of the cli connection (not just disconnecting out of the service using the "x" button). for instance, type "exit" at our command prompt closes the session and does remove the temp account.

- 5) (spfactory only- not available as spadmin): While logged into the CLI interface (not applicable to browser login), the TACACS username (same as the one in the addlocal file) will be displayed in **/etc** (to view, type **cd /etc** and type: **cat shadow**)

```
spfactory@Spectracom /etc $ cat shadow
root:!:1524075083:0:99999:7:::
halt:!:9797:0:!:!:
operator:!:9797:0:!:!:
shadow:!:9797:0:!:!:
sync:!:9797:0:!:!:
bin:!:9797:0:!:!:
daemon:!:9797:0:!:!:
adm:!:9797:0:!:!:
lpt:!:9797:0:!:!:
news:!:9797:0:!:!:
uucp:!:9797:0:!:!:
nobody:!:9797:0:!:!:
sshd:!:14700:!:!:!:
man:!:14700:!:!:!:
cron:!:14714:!:!:!:
ftp:!:14714:!:!:!:
dchp:!:14714:!:!:!:
quagga:!:14714:!:!:!:
stunnel:!:14714:!:!:!:
apache:!:14714:!:!:!:
ntp:!:14714:!:!:!:
ldsp:!:14714:!:!:!:
nullmail:!:14714:!:!:!:
fcrxon:!:14714:!:!:!:
mysql:!:14714:!:!:!:
tcpdump:!:14689:!:!:!:
messagebus:!:17554:!:!:!:
spfactory:01260000uk019szSRpaYZuQe0eubknhb.:17554:0:99999:7:::
spui:!:17554:0:99999:7:::
spadmin:01260000uk019szSRpaYZuQe0eubknhb.:17554:0:99999:7:::
spadmin:!:17639:0:99999:7:::
testusr:!:17639:0:99999:7:::
```

**Note:** exiting out of the cli interface (such as typing "exit" at our command prompt) removes the account name from shadow, very shortly thereafter.

In order to enable TACACS+ for ssh/pure-ftpd, a matching user account needs to be created locally on the SecureSync unit that matches the account on the TACACS+ server:

For example, a user with the username "user3" and password "pass3" on the TACACS+ server also has to create a "user3" account on the SecureSync unit before logging in (the password can be different).

**Reference information:**


- <https://en.wikipedia.org/wiki/TACACS>
- <http://www.cisco.com/ems/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius>

**TACACS+ Authentication**

HTTPS Security Level

Unlocking the Keypad

Secure Unit is Inaccessible



UTC: 2016-10-18 19:06:21

respective


The Server Status can be:

- **DISABLED** The TACACS+ service is disabled (see below to enable it)
- **UNREACHABLE** This TACACS+ server cannot be reached.
- **REACHABLE** This TACACS+ server can be reached

5. To **disable** a TACACS+ server from the list, click the X button in the Actions column

**Enabling/Disabling TACACS+**

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel on the left, click **TACACS+**. The **TACACS+ Setup** window will be displayed.



3. Check the box **HTTP/HTTPS**, and click **Submit** to enable **TACACS+** on this SecureSync. (Uncheck the box and click Submit to disable **TACACS+**).

➤ Radius Authentication in conjunction with TACACS and iPass is not supported.

## Enable/Disable TACACS and CLI commands available for TACACS

### A) Enable/Disable TACACS via web browser

- Refer to SecureSync user guide (excerpted below) at [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/TACACS.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm)

#### Enabling/Disabling TACACS+

To enable or disable the use of TACACS+ authentication on a SecureSync unit:

1. In the Web UI, navigate to MANAGEMENT > OTHER: Authentication.
2. In the Actions panel on the left, click TACACS+. The TACACS+ Setup window will be displayed.
3. Check the box labeled HTTP/HTTPS if you want to enable TACACS+, or uncheck the box if you want to disable TACACS+.
4. Click Submit.

### B) Disable TACACS (cant enable) via **resetpw** cli command (and 'resetpw' from front panel keypad/LCD)

*info below confirmed by Stuart on v5.8.2 (23 Jan 19)*

**resetpw** (via either the cli command or 'cmd' menu with keypad/LCD): **disables LDAP. Radius and TACACS** without changing any associated configs. These can be re-enabled via the browser after performing a **resetpw** command

#### Note about **servget** and **servset** cli commands:

These CLI commands **do not provide** ability to enable/disable TACACS, or to see if its enabled (as of at least v5.8.2, TACACS is not in the list of services which can be controlled via the CLI)

```
Spectracom NetClock 9483 Version 5.8.2
spadmin@10 ~ $ servget
Invalid arguments
Usage: servget <service>
  service: 0=daytime protocol service
           1=time protocol service
           2=telnet service
           3=FTP service
           4=SSH service
           5=HTTP service
           6=HTTPS service
           7=SNMP service
           8=NTP service
           9=Classic UI service
spadmin@10 ~ $
```

## TACACS operation

### TACACS login password is sent out unsecure (in the clear/not encrypted)

- Refer to Salesforce cases such as 165341 and JIRA ticket Number SSS-486
- This is the case in at least versions 5.8.0 and below

**Email from Mike Sutton (9 Jul KW)** The engineering team has reviewed the TACACS KEY displayed in clear text. It appears this is an issue due to debug levels being left on.

I am reaching out to Ryan J. in engineering to see when we can get the fix into an upcoming release. Possibly 5.8.1, but I have to confirm with engineering.

---

## Log entries associated with TACACS

- Auth log, Journal log (user log doesn't seem to log anything about TACACS)

### A) Journal log

- Per Keith- only one entry was asserted when I successfully configured/enabled TACACS on our unit  
Apr 11 18:24:46 Spectracom Spectracom: [WEB] Saved Tacacs Server data (spadmin)

---

### B) Auth Log

1. **“pam\_sm\_acct\_mgmt: returned attribute `PRIV\_LVL=15' from server” followed by “pam\_unix(useradd:auth): auth could not identify password for [spui]”**

- refer to Salesforce Case 177475

We may've found a subtle difference relating to authentication AND authorization using TACACS (these devices just care about authentication, but we're sending back both authentication and authorization)  
For the record, good vs bad logs:

- Prod (failing):

```
Nov 1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: active server is [204.27.45.5:49]
Nov 1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: sent authorization request
Nov 1 14:33:33 time512587gps01-new apache2[32096]: Args cnt 1
Nov 1 14:33:33 time512587gps01-new apache2[32096]: Adding buf/value pair (priv-lvl,15)
Nov 1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: user [<username>] successfully
authorized
Nov 1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: returned attribute
`PRIV_LVL=15' from server
Nov 1 14:33:33 time512587gps01-new apache2[32096]: pam_tally(httpd:account): pam_get_uid; no such user
Nov 1 14:33:33 time512587gps01-new apache2[32096]: pam_unix(httpd:account): could not identify user (from
getpwnam(username))
```

- Lab (working):

```
Nov 1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: active server is [204.151.176.210:49]
Nov 1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: sent authorization request
Nov 1 14:35:56 timel097771gps01 apache2[25307]: Args cnt 1
Nov 1 14:35:56 timel097771gps01 apache2[25307]: Adding buf/value pair (priv-lvl,15)
Nov 1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: user [username] successfully
authorized
Nov 1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: returned attribute `PRIV_LVL=15'
from server
Nov 1 14:35:56 timel097771gps01 useradd[31989]: pam_unix(useradd:auth): auth could not identify password
for [spui]
Nov 1 14:35:56 timel097771gps01 useradd[31989]: Authentication information cannot be recovered
Nov 1 14:35:56 timel097771gps01 useradd[31989]: failed adding user 'username', data deleted
Nov 1 14:35:56 timel097771gps01 useradd[32003]: pam_unix(useradd:auth): auth could not identify password
for [spui]
Nov 1 14:35:56 timel097771gps01 useradd[32003]: Authentication information cannot be recovered
Nov 1 14:35:56 timel097771gps01 useradd[32003]: failed adding user 'username', data deleted
```

2. **“pam\_sm\_authenticate: exit with pam status: 9” (note the number at the end can vary)**

- table below excerpted from: <http://pubs.opengroup.org/onlinepubs/8329799/chap5.htm>

## PAM Status Codes

PAM-API routines return PAM status codes as their int function value. These codes indicate major status errors that are independent of the underlying mechanism used to provide the security service.

| Name                        | Value in Field | Meaning                                                                              |
|-----------------------------|----------------|--------------------------------------------------------------------------------------|
| [PAM_SUCCESS]               | 0              | Successful completion.                                                               |
| [PAM_OPEN_ERR]              | 1              | Failure when dynamically loading a service module.                                   |
| [PAM_SYMBOL_ERR]            | 2              | Symbol not found in service module.                                                  |
| [PAM_SERVICE_ERR]           | 3              | Error in underlying service module.                                                  |
| [PAM_SYSTEM_ERR]            | 4              | System error.                                                                        |
| [PAM_BUF_ERR]               | 5              | Memory buffer error.                                                                 |
| [PAM_CONV_ERR]              | 6              | Conversation failure.                                                                |
| [PAM_PERM_DENIED]           | 7              | The caller does not possess the required authority.                                  |
| [PAM_MAXTRIES]              | 8              | Maximum number of tries exceeded.                                                    |
| [PAM_AUTH_ERR]              | 9              | Authentication error.                                                                |
| [PAM_NEW_AUTHTOK_REQD]      | 10             | New authentication token required from user.                                         |
| [PAM_CRED_INSUFFICIENT]     | 11             | Cannot access authentication database because credentials supplied are insufficient. |
| [PAM_AUTHINFO_UNAVAIL]      | 12             | Cannot retrieve authentication information.                                          |
| [PAM_USER_UNKNOWN]          | 13             | The user is not known to the underlying account management module.                   |
| [PAM_CRED_UNAVAIL]          | 14             | Cannot retrieve user credentials.                                                    |
| [PAM_CRED_EXPIRED]          | 15             | User credentials have expired.                                                       |
| [PAM_CRED_ERR]              | 16             | Failure setting user credentials.                                                    |
| [PAM_ACCT_EXPIRED]          | 17             | User account has expired.                                                            |
| [PAM_AUTHTOK_EXPIRED]       | 18             | Password expired and no longer usable.                                               |
| [PAM_SESSION_ERR]           | 19             | Cannot initiate/terminate a PAM session.                                             |
| [PAM_AUTHTOK_ERR]           | 20             | Error in manipulating authentication token.                                          |
| [PAM_AUTHTOK_RECOVERY_ERR]  | 21             | Old authentication token cannot be recovered.                                        |
| [PAM_AUTHTOK_LOCK_BUSY]     | 22             | The authentication token lock is busy.                                               |
| [PAM_AUTHTOK_DISABLE_AGING] | 23             | Authentication token aging is disabled.                                              |
| [PAM_NO_MODULE_DATA]        | 24             | Module data not found.                                                               |
| [PAM_IGNORE]                | 25             | Ignore this module.                                                                  |
| [PAM_ABORT]                 | 26             | General PAM failure.                                                                 |
| [PAM_TRY_AGAIN]             | 27             | Unable to complete operation. Try again.                                             |
| [PAM_MODULE_UNKNOWN]        | 28             | Module type unknown.                                                                 |
| [PAM_DOMAIN_UNKNOWN]        | 29             | Domain unknown.                                                                      |

Table 1. Routine Errors

### 3. “pam\_sm\_acct\_mgmt entries”

**Note:** refer to [https://linux.die.net/man/3/pam\\_acct\\_mgmt](https://linux.die.net/man/3/pam_acct_mgmt) (excerpted below)  
<http://www.xperientech.com/online/tacauthentication.htm>

- **PAM\_ACCT\_EXPIRED** User account has expired.
- **PAM\_AUTH\_ERR** Authentication failure.
- **PAM\_NEW\_AUTHTOK\_REQD** The user account is valid but their authentication token is *expired*. The correct response to this return-value is to require that the user satisfies the **pam\_chauttok()** function before obtaining service. It may not be possible for some applications to do this. In such cases, the user should be denied access until such time as they can update their password.
- **PAM\_PERM\_DENIED** Permission denied.
- **PAM\_SUCCESS** The authentication token was successfully updated.
- **PAM\_USER\_UNKNOWN** User unknown to password service.

**Note:** refer to: <http://www.xperientech.com/online/tacauthentication.htm>



## TACACS+ Specific Authentication

### START packet processing

- Authentication method is selected first by authentication type field from the packet.

#### Authentication action is selected.

- **TAC\_PLUS\_AUTHEN\_CHPASS** (that is "password change" request) and authentication method is not AT\_ASCII, ERROR packet is returned back to TACACS+ client.

#### If authentication method is AT\_ASCII and:

- a) If there's no user name in the packet, TAC\_PLUS\_AUTHEN\_STATUS\_GETUSER packet is sent back with a string prompting a user to input his name.
- b) If there's user name in the packet, TAC\_PLUS\_AUTHEN\_STATUS\_GETDATA packet is sent back with prompt to a user requesting his old password.

- **TAC\_PLUS\_AUTHEN\_SENDPASS** (that is "send clear text password to NAS" request) and TACACS+ minor version 0 support is turned off (defined by server configuration), ERROR packet is sent back.  
If no user name is present in the packet, ERROR packet is sent back.

- [ICommonAuthentication::GetUserPassword](#) is called next. If it indicates that there is no user known to server extension with such name, TAC\_PLUS\_AUTHEN\_STATUS\_FAIL packet is sent, and user is rejected.  
If user is found, but his password is not available in clear text or *ignorePassword* parameter is set to VARIANT\_TRUE, TAC\_PLUS\_AUTHEN\_STATUS\_FAIL packet is sent, and user is rejected. Otherwise, TAC\_PLUS\_AUTHEN\_STATUS\_PASS packet is sent back with user's password.

- **TAC\_PLUS\_AUTHEN\_SENDAUTH** and **authentication type is AT\_ASCII, ERROR** packet is sent back. Then server calls [ICommonAuthentication::GetUserPassword](#) to get user's password. If it is not available in clear text or no user exists with such name, TAC\_PLUS\_AUTHEN\_STATUS\_FAIL response is sent back, TAC\_PLUS\_AUTHEN\_STATUS\_PASS response is sent otherwise with authentication data dependant on authentication method.
- **TAC\_PLUS\_AUTHEN\_LOGIN**, [common authentication process](#) is initiated.

### CONTINUE packet processing

- If authentication method is not AT\_ASCII, ERROR packet is sent back.

#### If TAC\_PLUS\_CONTINUE\_FLAG\_ABORT flag is set, authentication process **terminates**.

- If action is **TAC\_PLUS\_AUTHEN\_CHPASS**

- If server extension does not know user name, old password or new password yet, it issues appropriate response with prompt to a user.

- If all authentication information is collected, server calls ICommonAuthentication::SetUserPassword.

- If action is **TAC\_PLUS\_AUTHEN\_LOGIN**

- If there's no user name in the packet, **TAC\_PLUS\_AUTHEN\_STATUS\_GETUSER** packet is sent back prompting auser to input his name.

- If there's user name in the packet, **TAC\_PLUS\_AUTHEN\_STATUS\_GETPASS** response is sent back with prompt to a user requesting his password.

- If server has both user name and password, common authentication process is initiate

## Note: log entries for web browser (apache) versus SSH login aren't the same

### 1) Apache web browser login using TACACS (ssh login is further below)

- "indented log entries below are TACACS-server related entries. Other entries are internal to SecureSync (such as ssh)

#### notes

testuser (in blue) is our correct TACACS account name

'spectracom\_test' (in brown) is our correct TACACS secret key

#### Actual Auth log entries from our unit with a successful login to the Apache web browser

**Aug 7 21:55:30 Spectracom apache2: pam\_succeed\_if(httpd:auth): requirement "user notingroup addlocal" not met by user "testuser" (note this is the starting entry for browser logging)**

```
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: 1 servers defined
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_service=""
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_protocol=""
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_prompt=""
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_login=""
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: user [testuser] obtained
Aug 7 21:55:30 Spectracom apache2[7567]: tacacs_get_password: called
Aug 7 21:55:30 Spectracom apache2[7567]: tacacs_get_password: obtained password
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: password obtained
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: tty [unknown] obtained
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: rhost [10.2.100.52] obtained
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: trying srv 0
Aug 7 21:55:30 Spectracom apache2[7567]: tacacs status: TAC_PLUS_AUTHEN_STATUS_PASS
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: active srv 0
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: exit with pam status: 0
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: 1 servers defined
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_service='ppp'
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_protocol='ip'
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_prompt=""
Aug 7 21:55:30 Spectracom PAM-tacplus[7567]: tac_login=""
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: called (pam_tacplus v1.3.8)
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: username obtained [testuser]
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: tty obtained [unknown]
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: rhost obtained [10.2.100.52]
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: active server is [10.2.100.4:49]
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: sent authorization request
Aug 7 21:55:30 Spectracom apache2[7567]: Args cnt 0
Aug 7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: user [testuser] successfully authorized
```

### C) Actual Auth log entries from our unit with Unsuccessful login using TACACS (right account name/bad password)

```
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: 1 servers defined
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_service=""
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_protocol=""
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_prompt=""
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_login=""
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: user [testuser] obtained
Apr 11 18:33:37 Spectracom apache2[28240]: tacacs_get_password: called
Apr 11 18:33:37 Spectracom apache2[28240]: tacacs_get_password: obtained password
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: password obtained
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: tty [unknown] obtained
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: rhost [10.2.100.52] obtained
```

```

Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: trying srv 0
Apr 11 18:33:37 Spectracom apache2[28240]: tacacs status: TAC_PLUS_AUTHEN_STATUS_FAIL
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: auth failed: 2
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: exit with pam status: 7
Apr 11 18:33:37 Spectracom apache2[28240]: pam_unix(httpd:auth): check pass; user unknown
Apr 11 18:33:37 Spectracom apache2[28240]: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001
tty= ruser= rhost=10.2.100.52
Apr 11 18:33:37 Spectracom apache2[28240]: pam_tally(httpd:auth): pam_get_uid; no such user

```

## 2) SSH login using TACACS

### 1. Successful login to ssh on our SecureSync (valid username and password)

- “indented log entries below are TACACS-server related entries. Other entries are internal to SecureSync (such as ssh)
- shown below as two “sets” of log entries- the first “set” after typing username <enter>, and the second set after typing password <enter>

#### A) First set of SSH login entries, after typing just the username <enter> (before entering a password)

```

Aug 7 21:27:51 Spectracom xinetd[2615]: START: ssh pid=22432 from=::ffff:10.2.100.52 (first entry for SSH)
Aug 7 21:27:59 Spectracom sshd[22703]: pam_succeed_if(sshd:auth): requirement "user notingroup addlocal" not met by user "testuser"
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: 1 servers defined
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_service=""
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_protocol=""
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_prompt=""
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_login=""
Aug 7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Aug 7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: user [testuser] obtained
Aug 7 21:27:59 Spectracom sshd[22703]: tacacs_get_password: called

```

#### B) Second set of SSH login entries, after typing password <enter>

```

Aug 7 21:27:51 Spectracom xinetd[2615]: START: ssh pid=22432 from=::ffff:10.2.100.52
Aug 7 21:27:59 Spectracom sshd[22703]: pam_succeed_if(sshd:auth): requirement "user notingroup addlocal" not met by user "testuser"
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: 1 servers defined
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_service=""
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_protocol=""
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_prompt=""
Aug 7 21:27:59 Spectracom PAM-tacplus[22703]: tac_login=""
Aug 7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Aug 7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: user [testuser] obtained
Aug 7 21:27:59 Spectracom sshd[22703]: tacacs_get_password: called
Aug 7 21:28:16 Spectracom sshd[22703]: tacacs_get_password: obtained password
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: password obtained
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: tty [ssh] obtained
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: rhost [10.2.100.52] obtained
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: trying srv 0
Aug 7 21:28:16 Spectracom sshd[22703]: tacacs status: TAC_PLUS_AUTHEN_STATUS_PASS
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: active srv 0
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: exit with pam status: 0
Aug 7 21:28:16 Spectracom PAM-tacplus[22703]: 1 servers defined
Aug 7 21:28:16 Spectracom PAM-tacplus[22703]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }

```

```

Aug 7 21:28:16 Spectracom PAM-tacplus[22703]: tac_service='ppp'
Aug 7 21:28:16 Spectracom PAM-tacplus[22703]: tac_protocol='ip'
Aug 7 21:28:16 Spectracom PAM-tacplus[22703]: tac_prompt=""
Aug 7 21:28:16 Spectracom PAM-tacplus[22703]: tac_login=""
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: called (pam_tacplus v1.3.8)
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: username obtained [testuser]
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: tty obtained [ssh]
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: rhost obtained [10.2.100.52]
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: active server is [10.2.100.4:49]
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: sent authorization request
Aug 7 21:28:16 Spectracom sshd[22703]: Args cnt 0
Aug 7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: user [testuser] successfully authorized
Aug 7 21:28:16 Spectracom sshd[22432]: Accepted keyboard-interactive/pam for testuser from 10.2.100.52 port 49779
ssh2
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: 1 servers defined
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_service=""
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_protocol=""
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_prompt=""
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_login=""
Aug 7 21:28:16 Spectracom sshd[22432]: pam_sm_setcred: called (pam_tacplus v1.3.8)
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: 1 servers defined
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_service='ppp'
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_protocol='ip'
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_prompt=""
Aug 7 21:28:16 Spectracom PAM-tacplus[22432]: tac_login=""
Aug 7 21:28:16 Spectracom sshd[22432]: _pam_account: [start] called (pam_tacplus v1.3.8)
Aug 7 21:28:16 Spectracom sshd[22432]: _pam_account: tac_srv_no=1
Aug 7 21:28:16 Spectracom sshd[22432]: _pam_account: username [testuser] obtained
Aug 7 21:28:16 Spectracom sshd[22432]: _pam_account: tty [ssh] obtained
Aug 7 21:28:16 Spectracom sshd[22432]: _pam_account: rhost [10.2.100.52] obtained
Aug 7 21:28:16 Spectracom sshd[22432]: _pam_account: connected with fd=6 (srv 0)
Aug 7 21:28:16 Spectracom sshd[22432]: _pam_account: [start] for [testuser] sent
Aug 7 21:28:16 Spectracom PAM-tacplus[23389]: 1 servers defined
Aug 7 21:28:16 Spectracom PAM-tacplus[23389]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Aug 7 21:28:16 Spectracom PAM-tacplus[23389]: tac_service=""
Aug 7 21:28:16 Spectracom PAM-tacplus[23389]: tac_protocol=""
Aug 7 21:28:16 Spectracom PAM-tacplus[23389]: tac_prompt=""
Aug 7 21:28:16 Spectracom PAM-tacplus[23389]: tac_login=""
Aug 7 21:28:16 Spectracom sshd[23389]: pam_sm_setcred: called (pam_tacplus v1.3.8)

```

## 2. Failed ssh login using TACACS to one of our secureSyncs (VALID account/bad password)

```

Apr 13 17:36:25 Spectracom sshd[15672]: Invalid user testuser\ from 10.2.100.52 port 64386
Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: 1 servers defined
Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_service=""
Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_protocol=""
Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_prompt=""
Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_login=""
Apr 13 17:36:25 Spectracom sshd[16150]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Apr 13 17:36:25 Spectracom sshd[16150]: pam_sm_authenticate: user [testuser\] obtained
Apr 13 17:36:25 Spectracom sshd[16150]: tacacs_get_password: called
Apr 13 17:36:25 Spectracom sshd[15672]: Postponed keyboard-interactive for invalid user testuser\ from 10.2.100.52 port 64386
ssh2 [preauth]
Apr 13 17:36:29 Spectracom sshd[15672]: Connection closed by invalid user testuser\ 10.2.100.52 port 64386 [preauth]
Apr 13 17:36:29 Spectracom xinetd[2383]: EXIT: ssh pid=15672 duration=13(sec)
Apr 13 17:36:33 Spectracom xinetd[2383]: START: ssh pid=16583 from=:ffff:10.2.100.52
Apr 13 17:36:41 Spectracom useradd[17005]: new user: name=testuser, UID=1003, GID=111, home=/home/spectracom,
shell=/bin/bash

```

```
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to group 'spadmin'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to group 'spuser'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to group 'addlocal'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to shadow group 'spadmin'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to shadow group 'spuser'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to shadow group 'addlocal'
Apr 13 17:36:42 Spectracom sshd[17061]: pam_succeed_if(sshd:auth): requirement "user notingroup addlocal" not met by user
"testuser"
Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: 1 servers defined
Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_service=""
Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_protocol=""
Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_prompt=""
Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_login=""
Apr 13 17:36:42 Spectracom sshd[17061]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Apr 13 17:36:42 Spectracom sshd[17061]: pam_sm_authenticate: user [testuser] obtained
Apr 13 17:36:42 Spectracom sshd[17061]: tacacs_get_password: called
Apr 13 17:36:46 Spectracom sshd[17061]: tacacs_get_password: obtained password
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: password obtained
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: tty [ssh] obtained
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: rhost [10.2.100.52] obtained
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: trying srv 0
Apr 13 17:36:46 Spectracom sshd[17061]: tacacs status: TAC_PLUS_AUTHEN_STATUS_FAIL
Apr 13 17:36:46 Spectracom PAM-tacplus[17061]: auth failed: 2
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: exit with pam status: 7
Apr 13 17:36:46 Spectracom sshd[17061]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=10.2.100.52 user=testuser
```

---

## C) User Log entries for TACACS

### 1. Successful login using TACACS

- Per Keith: I saw no User log entries asserted with a successful login

### 2. Unsuccessful login using TACACS (right account name/bad password)

- Per Keith: I saw no User log entries asserted with an unsuccessful login

---

## Troubleshooting issues with tacacs login/known issues

### A) General TACACS troubleshooting

1. Check the **Journal** and **Auth** logs (in the log bundle) for entries (user log does not seem to assert any entries for TACACS)
2. Make sure to try connecting/logging into both the web browser and a CLI service (such as ssh). With TACACS, browser login were handled differently than cli/ssh login:
  - **If both the browser and the cli/ssh login are failing:** Likely issue with TACACS account/tacacs server, or with the TACACS configuration (TACACS button on left side of **Management** -> **Authorization** page of browser)
  - **If browser login is working but cli/ssh login is failing:** Connection to the TACACS Server/TACACS account info in the TACACS server is likely fine. Probably an issue with the actual login name being typed (such as including domain info) or issue related to the 'addlocal' table. See info directly below
3. if the initial connection to the TACACS server(s) is failing, ask what type of TACACS server it is and ask for any logs in the TACACS server which may be asserted when the SecureSync tries connecting to it.
4. confirm the secret keystring is 100% correct.
5. Reboot the unit or stop/restart TACACS service

**Email from Ron Dries (15 Aug 2018)** Can you reboot this unit, when possible? Based on the configs you had provided us with, we believe just rebooting/power cycling the unit will restore normal TACACS functionality (as it was before the update was performed).

There is a file associated with TACACS, which is normally empty (except while logged in with TACAS). This file is also cleared on reboot. Since it was present in the saved config file you sent, we highly suspect the value entered into this file was either "restored" into the file during the update process to 5.7.1 (or if a previously saved config bundle happened to be restored sometime after the update was performed, the value was added back in at that time). With this one value already being present in this particular file when you login, TACACS isn't able to fully function as expected.

In summary, this file should be cleared with a reboot, and normal operation of TACACS should then be restored. Ron asked me to pass along to you that after rebooting, let us know that its operating normally again, and to also let us know if you ever happen to see the same condition occur again. Thanks in advance!

### B) Specific TACACS Troubleshooting

#### Software version related (What software version is installed in the SecureSync/9483?)

1. **(First observed/reported after v5.9.0 update) Tacacs users don't have permissions to perform CLI commands after updating from v5.8.9**
  - Refer to Salesforce Case 261853 (Nov 2020)
  - Refer to JIRA SSS-1142
  - Associated with at least versions 5.9.0, 5.9.1, 5.9.2, 5.9.3 and 5.9.4.
  - Refer to JIRA SSS-1142 (patch now available for v5.9.4). Refer to ("**SSH permissions in v5.9.4**") <\\rocfnp02\idrive\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches>

**Status update from Tim Hammer (12 Aug 2021)**  
RE: SSS-1142 (Salesforce Case 261853)

Thought I would just summarize our findings (recorded in ticket comments by Stuart) in case you want more details: We tracked the issue to an upstream change (in the sudo open source code) that we pulled in when we did the general/broad package update for 5.9.0.

The change "conflicts" with the way our cliwrapper commands works.  
Unfortunately, we have not identified a good way to handle the change on our side.

## 2. (First observed/reported with v5.8.9) Tacacs users are being cached

“...last minute testing on 5.8.9, I found an issue with tacacs authenticated users being cached on the appliance.”

- Refer to Salesforce Case 252722 (Nov 2020)
- Refer to JIRA SSS-1031.

---

## 3. (Applicable to versions 5.8.4 and 5.8.5) Memory leak causes Kernel lockup with “Tainted: G”, “Call Trace”, “page allocation stalls” and “out of memory manager” - due to TACACS

- Applicable to versions 5.8.4 and 5.8.5
- Fixed in update [version 5.8.6](#) (Oct 2019)
  - **Per the v5.8.5 Release Notes:** “Fixed an issue with TACACS+ and RADIUS causing kernel lockup, to improve responsiveness for SSH users.”

- Refer to SF Case 193787 and JIRA Ticket SSS-640

Delta Airlines and observed a v5.8.4 Kernel lockup (with 2nd gen ETX module installed) - “page allocation stalls” and “out of memory manager” - due to issue with TACACS

The unit locked up, Cant login and not responding to NTP. They have power cycled which has restored connection. and he is going to send me the logs. Needs to know why this has failed.

### Example kern.log entries

```
Sep 15 01:58:38kernel: [17963] 0 17963 923 426 3 0 0 0 sh
Sep 15 01:58:38kernel: [17969] 0 17969 625 439 3 0 0 0 userdel
Sep 15 01:58:38kernel: [17973] 0 17973 923 424 3 0 0 0 sh
Sep 15 01:58:38kernel: [17981] 0 17981 625 409 3 0 0 0 userdel
Sep 15 01:58:38kernel: [17993] 0 17993 923 402 3 0 0 0 sh
Sep 15 01:58:38kernel: [18000] 0 18000 625 410 3 0 0 0 userdel
Sep 15 01:58:38kernel: [18003] 0 18003 923 441 3 0 0 0 sh
Sep 15 01:58:38kernel: [18009] 0 18009 625 403 3 0 0 0 userdel
Sep 15 01:58:38kernel: [18012] 0 18012 923 424 3 0 0 0 sh
Sep 15 01:58:38kernel: [18017] 0 18017 625 406 3 0 0 0 userdel
```

```
Aep 15 01:58:38kernel: Out of memory: Kill process 4391 (php) score 43 or sacrifice child
Sep 15 01:58:38kernel: Killed process 4391 (php) total-vm:42456kB, anon-rss:19640kB, file-rss:3060kB, shmem-rss:0kB
Sep 15 02:01:57kernel: grep: page allocation stalls for 13944ms, order:0,
mode:0x14280ca(GFP_HIGHUSER_MOVABLE|__GFP_ZERO), nodemask=(null)
Sep 15 02:01:57kernel: CPU: 0 PID: 19502 Comm: grep Tainted: G O 4.14.34-gentoo #2
Sep 15 02:01:57kernel: Hardware name: /AMD-GX3, BIOS 6.00 PG 11/04/2008
Sep 15 02:01:57kernel: Call Trace:
Sep 15 02:01:57kernel: dump_stack+0x16/0x23
Sep 15 02:01:57kernel: warn_alloc+0xa5/0x130
Sep 15 02:01:57kernel: __alloc_pages_nodemask+0x695/0xa40
Sep 15 02:01:57kernel: handle_mm_fault+0x553/0xa40
Sep 15 02:01:57kernel: __do_page_fault+0x1c6/0x3f0
Sep 15 02:01:57kernel: ? vmalloc_sync_all+0x150/0x150
Sep 15 02:01:57kernel: do_page_fault+0xb/0x10
Sep 15 02:01:57kernel: common_exception+0x75/0x7a
Sep 15 02:01:57kernel: EIP: 0xb7d43c23
Sep 15 02:01:57kernel: EFLAGS: 00010202 CPU: 0
Sep 15 02:01:57kernel: EAX: 00021000 EBX: b7e90000 ECX: 00000000 EDX: 00496000
Sep 15 02:01:57kernel: ESI: b7e90780 EDI: 00000000 EBP: 00021001 ESP: bfc84a30
Sep 15 02:01:57kernel: DS: 007b ES: 007b FS: 0000 GS: 0033 SS: 007b
Sep 15 02:01:57kernel: ? vmalloc_sync_all+0x150/0x150
Sep 15 02:01:57kernel: Mem-Info:
```

Sep 15 02:01:57kernel: active\_anon:98828 inactive\_anon:67 isolated\_anon:0  
Sep 15 02:01:57kernel: active\_file:0 inactive\_file:921 isolated\_file:271  
Sep 15 02:01:57kernel: unevictable:0 dirty:3 writeback:0 unstable:0  
Sep 15 02:01:57kernel: slab\_reclaimable:326 slab\_unreclaimable:8469  
Sep 15 02:01:57kernel: mapped:850 shmem:104 pagetables:7647 bounce:0  
Sep 15 02:01:57kernel: free:1163 free\_pcp:52 free\_cma:0  
Sep 15 02:01:57kernel: Node 0 active\_anon:395312kB inactive\_anon:268kB active\_file:0kB inactive\_file:3684kB  
unevictable:0kB isolated(anon):0kB isolated(file):1084kB mapped:3400kB dirty:12kB writeback:0kB shmem:416kB  
writeback\_tmp:0kB unstable all\_unreclaimable? no  
Sep 15 02:01:57kernel: DMA free:1992kB min:88kB low:108kB high:128kB active\_anon:10508kB inactive\_anon:0kB  
active\_file:0kB inactive\_file:16kB unevictable:0kB writepending:0kB present:15988kB managed:15912kB mlocked:0kB  
kernel\_stack:584kB pagetables:844kB bounce:0kB free\_pcp:0kB local\_pcp:0kB free\_cma:0kB  
Sep 15 02:01:57kernel: lowmem\_reserve[]: 0 476 476

---

#### **4. Underscore symbol “\_” not allowed in Tacacs username (applicable to versions 5.8.6 to 5.8.8)**

- Refer to Salesforce Case 226714 (March 2020)
- Refer to JIRA ticket [SSS-886](#)
- Customer reported this issue after updating to 5.8.6
- fixed in version 5.8.9 update (June 2020)



## TACACS config files

### tacacs.conf file (in /etc)

- example below from a v5.8.0 unit with successful TACACS login working correctly

```
fcron          mke2fs.conf          sandbox.d
spfactory@Spectracom /etc $ cat tacacs.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.10
0.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
spfactory@Spectracom /etc $ █
```

### tacacs\_pam.conf file (in /etc)

- example below from a v5.8.0 unit with successful TACACS login working correctly

```
spfactory@Spectracom /etc $ cat tacacs_pam.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.10
0.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
spfactory@Spectracom /etc $ █
```

## TACACS Authentication (based on entries in the two conf files above)

- Refer to sites such as: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_tacacs/configuration/xr-16/sec-usr-tacacs-xr-16-book/sec-cfg-tacacs.html#GUID-7642CA69-B131-4F33-B626-7C49A83CA437](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xr-16/sec-usr-tacacs-xr-16-book/sec-cfg-tacacs.html#GUID-7642CA69-B131-4F33-B626-7C49A83CA437)
- **try\_first\_pass** causes **pam\_tacplus** to use a previously entered password, if one is available. If no password has been entered, **pam\_tacplus** prompts for one as usual.
- **service=PPP** “service” defines the ACACS+ service for authorization and accounting (in this case, its PPP)

**protocol=IP** “protocol” defines the ACACS+ protocol for authorization and accounting (in this case, its over the IP protocol)

**Note: ARAP and CHAP: don’t appear to be supported.**

---

**Specific TACACS known conditions:**

**A) (version 5.8.6 only) CLI command response: “You must be an administrator to invoke the model command”**

- Refer to Salesforce Case 217323 and JIRA Ticket SSS-748
- Software issue started in v5.8.6 and expected to be fixed in v5.8.7
- Affects both TACACS and RADIUS

---

**B) Can access SSH via TACACS, but not the browser (applicable to versions 5.8.2 and below)**

- Per the **v5.8.3** (Jan 2019) Release Notes “Fixed an issue in which **clean updates** wouldn’t allow TACACS+ access through http”

---

**C) Tacas password is sent in clear text (unsecure)**

- Refer to “**TACACS login password is sent out unsecure**” just a little ways up on this page.

---

**D) SecureSync is failing to initially connect to TACACS server(s) (even before TACACS account is authenticated)**

- Look at the Auth.log to see if the initial connection of SecureSync to TACACS server(s) (even before the credentials are checked) is failing. The following sequence of auth log entries will be asserted:

**apache2[2152] : tac\_authen\_read: short reply header, read 0 of 12: Operation now in progress**

**ilrlm600ntpcentral-m01 apache2[2152]: error communicating with tacacs server**

**ilrlm600ntpcentral-m01 PAM-tacplus[2152]: no more servers to connect**

**ilrlm600ntpcentral-m01 apache2[2152]: pam\_sm\_authenticate: exit with pam status: 9**

- **if the initial connection to the TACACS server(s) is failing ( entries below are in the auth logs), ask what type of TACACS server the customer is using, and ask for any logs in the TACACS server itself, which may be being asserted when the SecureSync tries connecting to it.**

---

**E) if SecureSync is successfully connecting to at least one TACACS sever(s), but login to a tacacs user account is not working at all (with neither the **Browser** or the **CLI/ssh**)**

**Note:** Always make sure to try logging in with both web browser and CLI connection (ssh) to see if both or only one of the two logins is failing.

As long as the SecureSync is able to initially connect to at least one TACACS server (“**user not authenticated by TACACS+” is not present in the auth.log**), if login with a tacacs account is not working at all (with nether the Browser, nor the CLI) and all the configs are correct, (correct username, password, worked in the past, etc.), TACACS SHOULD be working.

1. Reboot the unit and then try logging in again.

- **Per Stuart (5/24/17)** If login is succusful after just a reboot, let Stuart in Engineering know this happened (there is a very small chance a reboot will be needed to “clean up” some functions “running in the background”).

---

**F) Issue is only with **SSH** (login to **browser** with tacacs is working)**

- This indicates the “TACACS” account/login to the TACACS server itself is likely fine.

**1. Make sure software version 5.6.0 (or above) is installed**

- Verison 5..6.0 (or above) aded TACACS support for the CLI

- Before version 5.6.0 (version 5.5.0 was the only previous version with TACACS) TACACS only worked

with the web browser.

**2. This condition is likely related to the temporary username entry(entries) in the /etc/addlocal file (used for temporarily account name for ssh and other CLI services- this entry is not used with browser login).**

1. Verify the installed software is versions 5.6.0 or above (prior software versions allow TACACS connection to the browser only (addlocal was added in v5.6.0).
2. View the **/etc/addlocal** file in the configs bundle (or cat this file in **/etc**). It should contain only the user account name(s) (and some random numbers) of user tacacs account name(s) which have been used to connect via the cli/ssh. Examples below

**Below is an example of an expected addlocal file having only one TACACS user account**

```
e24988.1523579823
```

**Below is an example of an expected addlocal file having the domain name as part of the TACACS user account (preventing ssh connection)**

```
adprod\e23765.1521052953
```

3. View the **/etc/pam.d/ssh/default** file in the config bundle ???

Example from our working unit

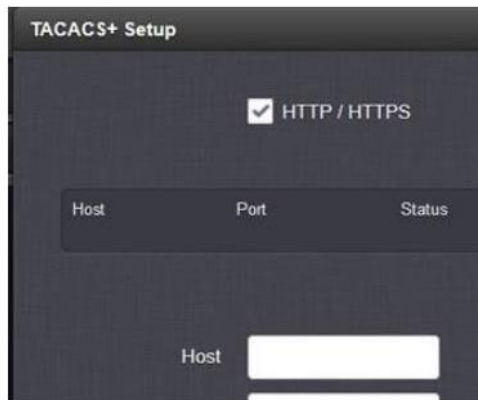
```
mpfactory@Spectracom /home/spectracom/config $ cd /etc/pam.d/
mpfactory@Spectracom /etc/pam.d $ cat sshd
# Default Version, no Radius or LDAP
session required pam_addlocal.so
auth include /etc/tacacs_pam.conf
auth required pam_unix.so try_first_pass
auth required pam_tally.so deny=5 unlock_time=60 per_user
account include /etc/tacacs_pam.conf
account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account required pam_deny.so
session include /etc/tacacs_pam.conf
session required pam_unix.so
session required pam_limits.so
session optional pam_lastlog.so
password required pam_unix.so shadow md5
mpfactory@Spectracom /etc/pam.d $
```

**After performing an upgrade to version 5.8.2 (or above) from a previous version 5.8.0 or 5.8.1**

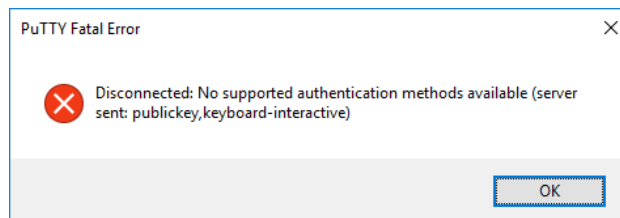
**(this is about the specific sequence requirement of the config file entries)**

- After updating to 5.8.2 (or above) from either versions 5.8.0 or 5.8.1 **SSH with TACACS may work fine**, while **browser with TACACS login** doesn't work. This is due to two lines in a config file being reversed during the earlier to newer software update process (not actually an issue in 5.8.2 or above) if a restore to defaults update is performed from versions 5.8.0 or 5.8.1
- The simple fix is to toggle TACACS off and back on (ensure the Submit button is pressed after unchecking the "HTTP/HTTPS" checkbox and then press submit a second time after re-selecting the checkbox). the order of the two lines is corrected when TACACS is disabled and then re-enabled.
- As I understood from Ron D (as highlighted in the above screenshot) The entry **"account include /etc/tacacs\_pam.conf"** has to be **BEFORE** the entry **"account required pam\_securetty.so"**
- Toggling TACACS off and back on switches the order of the two lines, if they are currently reversed
- Per SF Case 158734, if these two lines are reversed in the file, not able access the device through CLI while browser login works fine.

- fix is to disable/re-enable TACACS (make sure to press Submit after unchecking the box, and then press it again after selecting the box again- pressing submit a total of two times and no just once.
  - toggle the current state of TACACS (toggle it off and then back on again, using the “HTTP/HTTPS” checkbox at the top of the pop-up window for TACACS setup (**Management** -> **Authentication** page, **TACACS Setup** button on the left side) as shown below:



3. SSH login fails with a Fatal Error “**Disconnected: No supported authentication methods available (server sent publickey, keyboard-interactive)**”

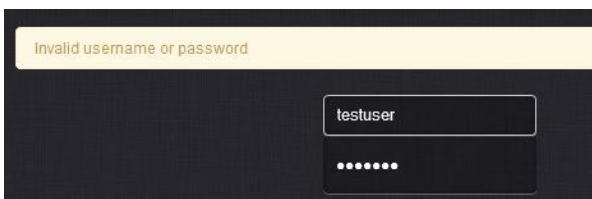


The SSH “Authentication Type” field (*Management* -> *SSH Setup* page of the browser) is likely configured as “Only Public Key”. When using TACACS, it needs to be set to either “Only Password” or “Public Key or Password”

SSH protocol versions supported (as of at least v5.7.1 and below): SecureSync supports SSH protocol version v2 only (not v1 or v3, as configured in /etc/ssh/ssh\_config)

4. SSH responds with “Access Denied” every time trying to connect with TACACS account
  1. Verify the TACACS account name is not also listed as an account created in the SecureSync (*Management* -> *Authentication* page of browser).
  2. Delete this TACACS user account if it’s listed.

(v5.8.0 and 5.8.1) TACACS login to **browser** fails (“invalid username or password”), **unless TACACS login to ssh is first performed**, and connection remains open- then login to browser. **SSH login with TACACS is fine.**



- Refer to SF cases such as 170655

- try rebooting the unit and try again

---

## **iPass**

- iPass is not available as of at least update version 5.9.5 (not aware of any plans to ever implement)
    - iPass requires specialized software from the iPass organization be installed, which is not currently possible with Spectracom time servers.
-

---

## Halt/Shutdown (software only) /System reboot/power cycle

### Upon a Halt, Network Processor Software (NPS) is stopped / KTS Timing System software continues operating

- Refer to Salesforce cases such as 166753 and 24195
- When a Halt or Halt/Shutdown is performed, the Network Processor Software (NPS) stops running (the web browser/CLI/ front panel display, NTP etc all stop working). However, the KTS timing system continues running after a Halt command has been performed
- Because the Timing System continues to operate after a Halt, unless the SecureSync is using NTP as its input (NTP stops running on a Halt), the SecureSync can remain in sync and Option Cards can continue providing outputs.

For example, the PTP Option Cards can continue indicating they are Clock Class 6 and providing useable PTP time stamps after performing a Halt command.

**Email Keith sent to NASA:** Your understanding of the Halt command is correct. With the exception of using NTP as the only input reference for the unit's synchronization (when using inputs such as either GPS or IRIG), the oscillator is still being disciplined and the rest of the timing functionality is still fully operational (the PTP card is still providing accurate and useable time) after the Halt has been performed.

*(Email excerpt from Case 166753)*

Below is some information you may find useful:

#### Upon a Halt, Network Processor Software (NPS) is stopped / KTS Timing System software continues operating

- When a Halt or Halt/Shutdown is performed, the Network Processor Software (NPS) stops running (the web browser/CLI/ front panel display, NTP etc. all stop working). However, the KTS timing system continues running after a Halt command has been performed.
- You will also continue to have your 1 PPS and 10Mhz as well.
- Because the Timing System continues to operate after a Halt, unless the SecureSync is using NTP as its input (NTP stops running on a Halt), the SecureSync can remain in sync and Option Cards can continue providing outputs.

For example, the PTP Option Cards can continue indicating they are Clock Class 6 and providing useable PTP time stamps after performing a Halt command.

---

## Differentiating between a reboot and a normal power cycle

(KW 27 Aug 2015) As of at least version 5.2.1, the only two differences I found between a power cycle and a reboot is

1. With a reboot (not a power cycle) the following two entries were asserted in the **kern.log** (they weren't asserted with a power cycle).  
Aug 27 11:37:52 custservice177 kernel: Kernel logging (proc) stopped.  
Aug 27 11:37:52 custservice177 kernel: Kernel log daemon terminating.
2. With a reboot (not a power cycle) the following entry was asserted in the user.log (it wasn't asserted with a power cycle).  
Aug 27 11:37:27 custservice177 shutdown[10762]: shutting down for system reboot

## Reboot

- Reboot can be performed via web browser, front panel keypad, CLI and SNMP (SNMP with software versions 4.8.8 and above)

### A) Reboot via CLI command

- The CLI command to reboot is “**reboot**”
- A new CLI command (added in version 5.3.1, Nov 2015) to reboot linux without potentially hanging it is “**reboot hard**” (refer to mantis case 3176)

### B) Reboot from front panel

- Front panel keypad reboot is via the System -> Cmd menus

### C) Reboot via SNMP

- Applicable to versions 4.8.8 and above

#### OID / Object to reboot (ssSysCtrlCommand)

**Note:** ssSysCtrlCommand was added in software version 4.8.8. (Not available in versions 4.8.7 and below)

| OID            | Name             | Function                                       | Value to “Set”                                                                                                      |
|----------------|------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| 8837.3.2.2.5.1 | ssSysCtrlCommand | Either Reboot or apply remote software updates | “4” to reboot<br><br>(SNMP Get will normally return “idle (1)”. Values 2 and 3 are for performing software updates) |

---

## Halt/Shutdown (Halt and shutdown) and Clean/Halt (Clean and Halt)

### Note about clean/halt (clean and Halt)

- **per the v5.9.0 Release notes:** The “Clean and Halt” command does not function properly when logged into SSH

**Halt** (shutdown) can be performed via web browser, CLI commands, front panel keypad, or SNMP:

#### A) Via newer web browser (v5.1.2 and above)

- Halt is located in the [Tools](#) -> [Reboot/Halt](#) page of the newer black/charcoal browser.

#### B) Via CLI interface

- CLI command to halt without cleaning/resetting configs is “**halt**”
- CLI command to halt with cleaning/resetting configs is “**cleanhalt**”

#### C) Via front panel keypad

- Front panel keypad halt is via the **System** -> **Cmd** menus

## D) Via SNMP

- **Reboot** is available via SNMP starting in update version 4.8.8 (see info above).
- **Halt/Shutdown** is not available via SNMP (as of at least version 5.1.5):

Q (general question from various customers: "Do I need to halt the time server before powering down?")

**A draft Email Keith has sent** This is a very good question, and I have some information for you that I hope will help alleviate any concerns that you may have about this:

Like any other computer, it is always best to stop the programs that are currently running before just pulling the power cord out of the computer. Otherwise, there is always that small chance that you could corrupt a program this was running at power down. So, computers usually internally stop all processes before they power-down, just to be safe. The HALT command is the method used to stop all processes in the SecureSync before powering power.

The Halt Command is provided to promote file system stability. It does take time to preserve data in the file system. Using halt to shutdown the SecureSync rather than just removing power ensures log data, and configuration information being written to the file system is successfully stored. Also, it avoids any issues of file system corruption. The file system can recover from corruption and errors. However, to avoid file system corruption the use of Halt is recommended. Also if a file error was to occur, the file system will try to fix it the next time the unit is booted up. This process could cause the power-on to take longer than normal.

Q. Is there any SNMP or other API call that will shut the system off? The web interface is close but I don't like the idea of screen-scraping the web-response to determine when the system is ready for a power. Is there a simple C or java blocking call or system command we can invoke to do this, with response saying if it did shut down or pulled an error?

A In addition to the web browser interface, the SecureSync can also be shut-down (halted) via the front panel keypad or via the CLI interface (such as the front panel RS-232 SERIAL port, telnet or SSH). The CLI command to cause the shut-down is "**halt**". The halt command is discussed in Section 3.8 (starting on page 3-21) of the attached SecureSync manual. It's also listed in the available CLI commands section (Section 11).

Once the halt has been performed, all processes are stopped. Since there is no way to send an indication when all processes have been stopped, the SecureSync itself cannot indicate it has been halted. However, it can be confirmed as being shut-down by trying to contact it after about 20 seconds or so with any network method. Once halted, SNMP, ping, etc will fail. An SNMP Manager will also show it no longer responding. Once the halt has been issued, it will shut-down completely shortly thereafter.

## Upon performing HALT/Shutdown

### Once Halt has been performed

#### 1. 1PPS output and 10MHz outputs

- (we confirmed this here with our unit) 1PPS output and 10MHz outputs (hardware outputs) continue to be present after performing a halt.
  - Halt is a software-only shutdown. It does not shutdown the hardware, hardware outputs such as 1PPS and 10 MHz continue to be outputted as long as power is applied- they are not stopped if the software is not running (even if Signature control is enabled, because Signature Control is a software function).

#### 2. The front panel LED time will stop counting up???

Per Case 289246 (Nov 2022) TOYO reported in versions 5.9.4 and below, the time stops incrementing. But in version 5.9.5, the time continues to increment?? I was not able to duplicate this with my v5.9.5 SecureSync. Halted it twice, and both times the front panel LED clock froze/stopped incrementing.



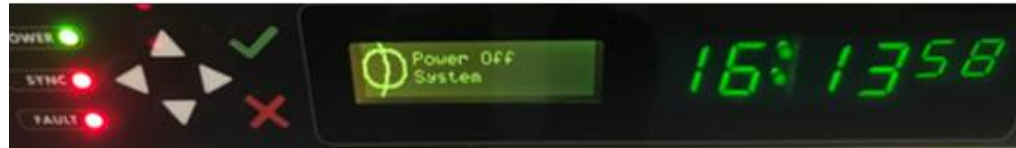
### 3. The front panel LCD:

A) With newer 2<sup>nd</sup> generation (64 bit) ETX module installed) will display a blank screen

Email from Ron Dries to Dave L (27 Nov KW) SecureSync server with the newer 64 bit ETX module do not display the "Power Off System" message.



B) With 1<sup>st</sup> generation (32 bit) ETX module installed): will display "Power off System"



### 4. A broadcast message is sent to the CLI interfaces

Broadcast message to CLI interfaces when Halt/Clean Halt is performed.

```
cal: illegal year value: use 1-9999: 'ls'
spadmin@Spectracom ~ $ ca
Broadcast message from root@Spectracom (Tue Jul 30 20:51:48 2013):
The system is going down for reboot NOW!
```

## Report of SecureSync appearing to have rebooted itself

- This may be a misconception due to a graceful restart of the Apache web browser and the associated log entry that is asserted.
- Refer to "Graceful Restart" in the HTTPS Section of this document (just search for this term).
- It could also be related to "preemption" being enabled in Linux (software update versions 5.3.1 and below). Preemption was disabled in version 5.4.0. See info below.

## Linux preempt/preemption (potential cause of lock-ups/ system hanging??)

- Preemption (preempt) was enabled in the Linux kernel with software update versions 5.3.1 and below
- It was disabled/turned-off starting in software update version 5.4.0
- "preempt" has often been found in the kern.log along with oops, call trace and other error messages.
- Engineering found reports from others that preempt being enabled in the linux kernel can cause problems. So it was disabled starting in 5.4.0 as a potential fix to issue that Verizon and others may be experiencing.

### Likely fix- version 5.7.0

\* [JIRA Ticket SSS-272] – "Bug in Gentoo 4.0.5 kernel: periodic call traces"

---

## **\*\*Parallel Redundancy Protocol (PRP)**

**Q. Email from Mark Day regarding question from Aimil** -Could you please advise on Sunil's question below regarding support of the Parallel Redundancy Protocol in the SecureSync? I can find no mention of it on the datasheet or in the manual. My understanding is that identical data packets are sent out over two separate networks and assumed to be fail independent, allowing for zero-time recovery and check the redundancy continuously to detect lurking failures on the network as long as one network is operational– is that correct?

**A. Reply from Dave Sohn (3 Apr 2013)** We do not support parallel redundancy protocol in SecureSync.

---

## **\*\*IPSec (IP Security)**

For general/troubleshooting info on IPSec, refer to: [IPSec / IP Security \(for all products\)](#)

[S:\Engineering\Projects\Lafayette\300 Verification Test Plan\Integration Test Plans\LIT\\_030\\_IPSec.doc](S:\Engineering\Projects\Lafayette\300 Verification Test Plan\Integration Test Plans\LIT_030_IPSec.doc)

[S:\Engineering\Projects\Lafayette\301 Verification Test Results\2010 May Release\LIT Documents\LIT\\_030\\_IPSec\\_2010\\_05\\_13.doc](S:\Engineering\Projects\Lafayette\301 Verification Test Results\2010 May Release\LIT Documents\LIT_030_IPSec_2010_05_13.doc)

<S:\Engineering\Projects\Lafayette\301 Verification Test Results\IPSec\Testing IPSec for Lafayette.docx>  
<S:\Engineering\Projects\Lafayette\301 Verification Test Results\IPSec>

[..\Engineering\Engineering\\_Shared\Security\Interpeak ipsec.pdf](..\Engineering\Engineering_Shared\Security\Interpeak ipsec.pdf)

**Important Note (KW):** IPSec was removed in the **Version 5.1.2** upgrade. As of Feb 2014, it's still undecided whether or not it will be added back in, with a future update.

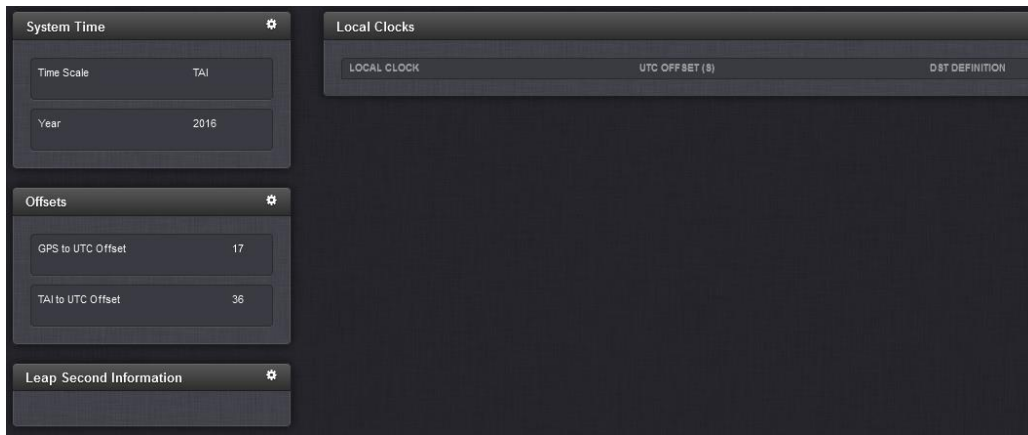
- SecureSync supports IPSec.
- IPsec is configured in the Network -> IPsec page of the web browser.

## Time Management (System Time, GPS/TAI Offsets, local clocks)

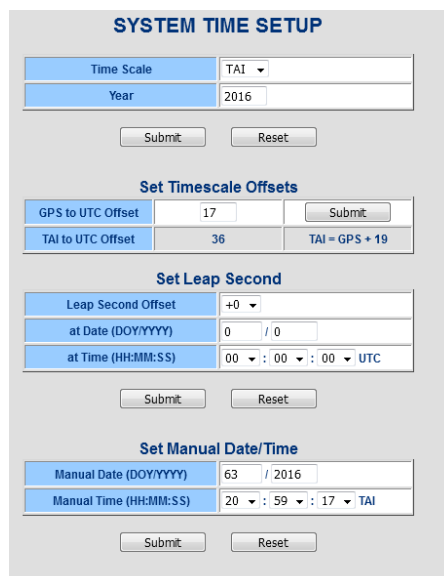
### \*\*System Time/Year and System timescale

System Time is configured in the:

#### A) Newer browser: Management -> Time Management page of the browser

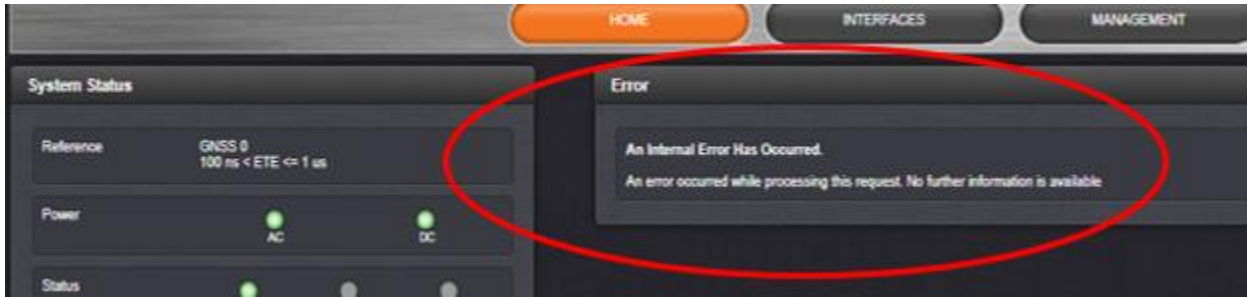


#### B) Classic interface: Setup -> Time Management page of the browser



**Error message: “An internal error has occurred...”** is displayed **ONLY** while navigating to **JUST** the **Time Management** page of browser (all other pages of the browser navigate without an error message)

- Full error message displayed: **“An internal error has occurred. An error occurred while processing this request. No further information is available”**
- On at least one occurrence (18 Dec 2018, with v5.5.1 installed), this error message (An internal error has occurred...) was displayed **ONLY** when trying to navigate to **JUST** the **Management -> Time Management** page of the browser. All other pages were navigating just fine, with no errors displayed (recommended they reboot it-see the “software crash” email below).



## Potential Solutions

- Software crash with earlier versions such as v5.5.1

**Email from Dave L (8 Jan 18)** The Internal Server Error may be caused by a crash of the web service in the 9483. This can happen on rare occasions in older firmware versions such as 5.5.1. Typically a power cycle will restart the web service and restore communications.

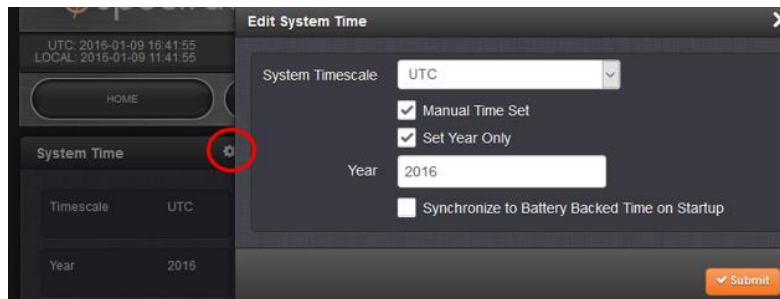
Updating the firmware will help prevent this from happening in the future. We recommend updating to the latest version 5.7.1 which is available for free from our website. Here is a link to download the update and instructions.

<https://files.spectracom.com/public-downloads/latest-securesync-netclock-files>

IF the power cycle does not restore the web browser please let me know and we can explore a solution or RMA this 9483.

## System Year / “Set Year Only” checkbox/field

- With the exception of IRIG input having no year (such as B000), the year is normally set by the input reference.
- “Set year only” Checkbox/field is used when an IRIG input reference doesn’t contain present Year.
- Based on testing, the “**Set Year Only**” year value does persist during system reboots/power cycles (in case of power cycles, as long as the year is set at least 10 minutes before power cycle, so that the RTC has a chance to be updated). Reboots and Halts update the RTC automatically, at the time they are performed.



1. **Management** -> **Time Management** page and press the gear icon to the right of “**System Time**”
2. Select “**Manual Time Set**”
3. Select “**Set Year Only**”
4. Change the Year, as desired, and then press Submit (don’t need to also select “synchronize to battery backed...”)
5. With the system synced via IRIG input, can either perform a reboot command (via the browser, CLI or front panel) or wait at least 10 minutes after changing the year for the RTC to be updated, before power cycling.
  - If the unit doesn’t run long enough (up to 10 minutes) after setting the year before its power cycled, the year will be set to the earlier configured year once its boots-up. The RTC is only periodically set (every 10 minutes or when a reboot is commanded). RTC is set on commanded reboot, so no delay is necessary when rebooting.
  - See additional info further below

### CLI commands to obtain/change the System Year

**yearget**

**yearset xxxx**

```
2021
spadmin@Spectracom ~ $ yearset 2020
spadmin@Spectracom ~ $ yearget
2020
spadmin@Spectracom ~ $
```

**Delay of up to 10 minutes is needed after changing the year to set the RTC, before power cycling.**

- Refer to SF case 123677

**Email Keith sent (9 Jan 18)** I just worked with one of our Apps engineers to more closely duplicate your same scenario of IRIG B000 input (I performed a quick test without an IRIG input applied).

He had a SecureSync outputting IRIG B000 to another SecureSync, with both set to year “2018”. He then changed the “**Set Year only**” field in the Slave SecureSync to “**2017**”, and then **rebooted** via the web browser the Slave SecureSync. The Slave SecureSync then powered-back up with the year value still set to the value of “**2017**” as expected.

We want to first confirm the version of software currently installed in the IRIG Slave (as reported in the Tools -> Upgrade/Backup page of its browser). This is not likely a factor, but just want to make sure. If I recall correctly, I believe it's the latest version of version 5.7.1.

We may end up needing the logs and configs files. But as I realize this can be very difficult, one other factor that we can also review first, as this can affect this field, is the actual test process and durations between steps.

The test we performed used a "graceful" shutdown/restart of the Slave SecureSync (as commanded with the **Tools -> Reboot/Halt** page of the browser, and selecting the "**Restart after Shutdown**" checkbox.

Note that when you manually change the year value, just submitting the change doesn't immediately set the Real Time Clock (RTC) which is used for the initial time/date/year at startup of the system. The RTC is only set periodically, or when a Halt/reboot (graceful shutdown) has been commanded. If the system is just power cycled (instead of being commanded to reboot) too soon after changing the year, the newly set year value will not be set to the RTC, and therefore will not be used at the next boot-up (it will revert back to the year that was set before it was manually changed).

For your testing, was the SecureSync rebooted via the browser or instead power cycled? Also, how long after changing the year did the unit continue to run thereafter, before it was rebooted/power cycled? Just moments later, or several minutes later (at least 10 minutes before a power cycle was performed)?

If testing with a loss of power, the unit needs to be running long enough after setting the year, for the periodic routine which sets the year in RTC to have been performed again. As its performed every 10 minutes, if the unit is not commanded to reboot, and is instead power cycled, and unless you first check to see when the RTC has been set, you will need to wait at least 10 minutes after setting the year before power cycling, in order for the RTC to contain the new year, and to have it boot-up with the correct year value.

To ensure the RTC has been changed to the new year value before rebooting or power cycling, open an ssh session and perform a `date <enter>` cli command. Once this command starts showing the newly set year value (in place of the earlier year), the RTC has now been updated and the unit will use this new year value upon its subsequent boot-ups.

FYI- instead of just typing 'date', if you type `watch -n1 date <enter>` you can see each second when the year has been set in the RTC, indicating it can then be power cycled (this alleviates needing to keep typing date, as it will refresh the date each second).

Our testing is showing the Set Year for IRIG input is operating as expected. Let me know if you observe anything different (the operational time required after setting the year- before power cycling - explains why you were "sometimes" seeing the expected results. These times, the unit likely ran long enough after setting the year for the RTC to be set, before it was subsequently power cycled).

### **Year rollover with IRIG input, if the SecureSync has been "Halted" before/during the transition from 31 Dec to 1 January (New Year Rollover)**

- Refer to TOYO Salesforce Case 256666
  - A v5.8.4 SecureSync with IRIG Input only (year not provided in IRIG signal) was halted on 18 Dec 2020, and not booted-up again until 12 January 2021. When powered back up, 12 days after year rollover, Year was still set to the previous year value of 2020.

### **Keith's simulated testing of "Set Year Only" Year Rollover (using IRIG input, no year provided) for Halt testing**

1. With the IRIG slave (V5.8.9 SecureSync) remaining powered-up ("**Set year only**" to "2020") and syncing to the IRIG master during the New Year Rollover, the IRIG slave properly incremented on its own to 2021 at UTC midnight
2. With the same IRIG slave ("**Set year only**" to "2020" and "**Battery backed time**" not selected) initially syncing to the IRIG master (starting about one hour before the New Year Rollover), and then the IRIG slave was Halted about 30 minutes before UTC midnight (so that it would still be halted at UTC midnight) the IRIG slave properly incremented on its own to 2021 at UTC midnight

| Id | Date               | Entity  | Message                                 |
|----|--------------------|---------|-----------------------------------------|
| 86 | Dec 31<br>23:33:32 | [WEB]   | The system is being shutdown (spadmin)  |
| 85 | Jan 01 00:35:21    | [webui] | Set Year for Clock slot 0 to Year: 2020 |

UTC: 2021-01-01 00:39:28

## System Timescale

- System Time is UTC timescale by default
- Can be changed to either TAI or GPS timescale as desired (press the gear icon next to “System Time”):



- Changing the System Timescale value changes the “System Time”. So all references to time with the exception of PTP output (outputs such as the front panel, browser, NTP, logs, etc) use the new timescale offset.
- As of at least software version 5.4.1, NTP (and the unit’s logs) doesn’t have its own individual timescale configuration, so it will always follow the System’s timescale.
 

Besides NTP, other inputs/outputs (such as ASCII and IRIG for examples) have their own individual timescale configurations available. So for instance, the System timescale can be set to UTC, but IRIG can be outputted as either GPS or TAI.
- PTP Option Cards always read the System Time in UTC timescale, no matter what timescale is selected. It always outputs TAI (if the UTC to TAI offset is set correctly). The 1204-12 and 1204-32 cards can’t be configured to output any other timescale except TAI.
- Timekeeper software (with the timekeeper license installed) outputs time in UTC timescale (timekeeper software doesn’t always follow the PTP standards).

## Affect on NTP when the System Timescale is changed to a different value

- ntpmond should automatically stop and restart NTP due to the larger than one second correction.
- Sample log entry from version 5.4.0 (NTPv4.2.8p6) when changing TAI back to UTC: `0.0.0.0 0413 03 spike_detect -35.999985 s`

## Timescale configuration of certain input references can affect the System Time, even if the System timescale is set as desired.

- References such as IRIG, RS-232, RS-485, etc can provide the SecureSync with time in a difference timescale or offset than the System timescale is set to.
- When this is the case, the input reference needs to be properly configured with the timescale/offsets being supplied so that the System know how to properly convert the time its receiving to be in the correct timescale that the system is configured to operate in.
- For example, if the IRIG source is providing TAI timescale. It needs to be configured to report its receiving-providing TAI time.

## \*\*GPS Offset (Antenna Cable Delay/ACD) (AKA GNSS Receiver Offset)

- Provides a “group of all outputs” delay/advance configuration (instead of using individual output delay compensation)
- When configuring the antenna cable delay for a SecureSync, you want to use "+" (or no sign entered) . This will advance/forward the System PPS by the same amount the cable is going to inherently "retreat/retract" the 1PPS Offset.

Refer also to “**GNSS Receiver Offset**” in the online 1200 SecureSync user guide at:

[https://orolia.com/manuals/SS/Content/\\_Global/Topics/GNSS/GNSS\\_recOffset.htm?Highlight=cable%20delay](https://orolia.com/manuals/SS/Content/_Global/Topics/GNSS/GNSS_recOffset.htm?Highlight=cable%20delay)

### Whether to use a positive (+) value or a negative (-) offset value (from Case 259422, discussing IRIG output OFFSET)

**Email from Keith** Adding delay (Offset) compensation on the input reference that the SecureSync is synced with (such as GPS or IRIG input) will inherently move the SecureSync's System 1PPS and all its outputs by the Offset value entered (a positive value to push the 1PPS ahead, or negative to pull the 1PPS back). But if its desired to only offset one particular output (such as an IRIG output), the Offset should be configured for just that particular output.

A positive Offset value will "advance/forward" the 1PPS, while a "negative" Offset value will "retreat/retract" the 1PPS Offset. So, adding a positive 27000 ns Offset in the dedicated IRIG output going over to the other SecureSync will advance the 1PPS its providing by 27 microseconds. Adding a negative "27000" ns Offset will retreat the 1PPS of the IRIG by 27 microseconds.

If the 27 microseconds of offset is due to the coax cable delay between the IRIG out of the GPS-synced SecureSync to the other SecureSync, adding a positive 27000 ns of Offset to the IRIG output (Interfaces -> IRIG out page of the web browser) will "advance" the 1PPS of the IRIG output by 27 microseconds.

When the IRIG output signal reaches the secondary SecureSync, the advancing of the PPS (inside the GPS SecureSync) will have then been negated at the input of secondary SecureSync by the actual delay through the cable, resulting in the PPS of the IRIG output and the PPS of the IRIG input coincident with each other (as if they were directly connected to each other, instead of having a cable located between them).

### Calculating Antenna Cable Delay values (Coax or Fiber)

- Refer to “1PPS / Antenna cable delay calculations” in <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>

### Entering the calculated value into the SecureSync

#### A) New web browser

- **Management** -> **Time Management** page of the browser
- Click on the “gear” icon next to “Offsets” (left side of the page)



From the SecureSync user manual, cable delay can be set to a max of + /- 50 milliseconds (entered as 50,000,000 nanoseconds).



## B) Classic Interface:

- GPS Antenna cable delay is configured in the Setup/Inputs/On Board Reference GPS page of the browser.
  - From the SecureSync user manual, cable delay can be set to a max of +/- 50 milliseconds (entered as 50,000,000 nanoseconds).
- 

### **\*\*“GPS to UTC offset” (Number of leap seconds)**

#### **Reported in:**

- Newer browser: [Management](#) -> [Time Management](#) page

#### **Automatic updating of this value**

- This value is only automatically updated if GPS changes its data message to indicate it's now a different value.
- It's the change in the GPS message (a leap second occurring) that automatically updates this value in the time server.
- If the value is manually changed to an incorrect value while GPS is present, or if GPS is subsequently reconnected, GPS WON'T simply correct the value. It will need to be manually corrected or it will remain set to the incorrect value.

### **UT1 (GPS to UTC offset) is now stored in SecureSync for faster GPS sync**

UT1 offset is now stored after the first time that the GPS receiver downloads the UT1 offset value from the 12.5 minute ephemeris data (the first time after it's been cleaned, its stored).

Special release Version 4.5.N introduced the ability for the UT1 offset to persist through power cycles.

- This new capability was officially cut-in with the version 4.7.0 software update.
- This capability reduces sync to GPS time to about 2 minutes or so after power-up.

### **Software Version 4.5.N for faster GPS sync**

#### **Email from Dave Sohn (7/17/11) regarding this pending special software release:**

I finished the SW patch (SecureSync version 4.5.N) and initiated sign-off (ECN 2707) to release. This improves NTP and GPS startup synchronization times. Total time from startup to GPS sync is about two and a half minutes. Total time from startup to NTP Stratum 1 sync is about five minutes. Some caveats, though. In order for the fast NTP sync, after the unit is updated, a factory clean should be performed to make sure the NTP configuration files are set properly. The unit needs to know the UTC/GPS offset in order for the GPS fast sync to work. That means that the unit must have been synchronized to GPS with the normal startup time once, including performing survey if GPS is in stationary mode. Each startup after that, the GPS can utilize the faster sync time.

---

### **Leap Years (Leap Days)/February 29<sup>th</sup>**

- Refer to Salesforce Case 222516

Q “Does Spectracom have any official documentation regarding Leap Days and how these are handled?  
We know it will not be an issue, but we have internal customers who would like something in writing”

---

## \*\*Leap Second insertion

- For general info on NTP handling leap seconds, refer to: [Leap Seconds](#) (in CustomerServiceAssistance.pdf)
- Refer also to the draft SecureSync email from the 2015 leap second: [..\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\leap second](#). First part is about NTP and the second is about PTP.

### General info

- The GPS receiver automatically flags leap second to occur on last second of the last day of the month (typically either last day of June and/or December)
- GPS typically announces leap second at least 30 days prior to insertion but no more than 6 months prior to insertion.

---

### Next scheduled leap second flagged in the system

- CLI command to obtain the next scheduled leap second: **CS\_getLeapSec 0**
- Next scheduled leap sec is displayed in the **Mangement** -> **Time Management** page of the newer browser.
- Once a scheduled date is "in the past", it no longer affects the system operation

---

### Changes in outputs to indicate the Leap second is pending:

- **NTP** changes LI bits (Leap Indicator bits) **24 hours** prior to leap insertion (initially 00 and then change to "01")
- **PTP** changes Announce message **12 hours** prior to leap insertion
- **IRIG** output changes data **1 hour** prior to leap insertion

**Note:** The **IEEE-1344 extensions** need to be enabled on the IRIG output and the IRIG input to pass leap second pending info to an IRIG slave. For more info on 1344 extensions, refer to: [..\CustomerServiceAssistance.pdf](#)

---

### NTP flags leap second insertion even with just one upstream NTP server indicating leap second is pending (versions prior to version 4.2.6)

- Reportedly, in NTP versions prior to version 4.2.6, NTP will insert a leap second at the end of the month even if only one NTP server announces a leap second is pending
- Refer to [https://groups.google.com/forum/#!topic/comp.protocols.time.ntp/nHZOEvNTpVo\[1-25\]](https://groups.google.com/forum/#!topic/comp.protocols.time.ntp/nHZOEvNTpVo[1-25])
  - "The other is in pre 4.2.6 versions that they accept the leap at any time when any of its sources is announcing the leap"
  - "The current firmware version, 6.18.004, ships with NTP 4.2.8p3 which doesn't accept a leap second announcement from a single upstream server."

---

### "Leap smear"/ Desire to slew the time for leap second (like Google now does) instead of an "immediate" correction

- Refer to NTP documentation: <https://docs.ntpsec.org/latest/leapsmear.html>
- Refer to Google documentation: <https://developers.google.com/time/smear>
- As of at least 5.8.9 and below, this functionality is not currently available in standard SecureSyncs (using ntpd software)
- Suspect this capability is available by purchasing/installing Timekeeper option (SS-OPT-TKL) which replaces NTPd when enabled.

- FSM has implemented this function into their software to allow either a slew or immediate correction. ~~So it would be available with the Timekeeper license, if its purchased and installed (our P/N SS-Opt-TKL. Refer to <https://na8.salesforce.com/01tC0000004KDut?srPos=13&srKp=01t> for additional info on this available purchasable Option).~~

## Goggle's public NTP service (which performs "leap smear")

➤ Refer to case 233585

Q We would like to know if this appliance/software combination can be peered with Google's public NTP service. Our primary time source is GPS, but we would like to use a reputable NTP server on the internet as a backup. Reading Google's documentation on <https://developers.google.com/time/faq>, they mention that they do "leap smear" and have a warning about some system not properly supporting that. Is this supported on our Spectracom?

**A Per Ron Dries:** Our NTPD is not built to support leap smearing, although this only really impacts how we serve time it means that as a client we are setup to use a leap seconds file which when synchronizing to a leap smearing NTP server will cause the leap second to be applied twice. Found this information in section 5. Using NTP's Leap Second Smearing from this link: <https://docs.ntpsec.org/latest/leapsmear.html>

I would be concerned with the interaction between the GNSS reference and NTP. GNSS will announce the leap second and we will apply it by using a jump when it occurs. When smearing the leap second NTP does not notify of the coming leap second because it will be applied gradually. If they have some systems on GNSS and some running NTP during a leap second then there absolutely could be a mismatch between them.

I believe we would recommend using a NIST NTP server, or the NTP pool servers as an internet time backup.

**Keith's response to customer:** In summary of the info below, we do not recommend peering a SecureSync with a time server which will perform "leap smearing" in the event of any potential, future leap seconds being asserted. Instead, we recommend peering Securesyncs with only other NTP servers that have NTP handle leap seconds in its standard fashion (NTP servers sending its clients a leap second pending indication via its LI bits),

Per our Engineers, the SecureSync is not intended to be peered by another time server that is performing leap smearing...

Our NTP functionality doesn't support leap smearing, although this only really impacts how the SecureSync serves time to its NTP clients. It means that as an NTP client (when the SecureSync is only synced via NTP input), the SecureSync is setup to use an NTP leap seconds file, which when synchronizing to a leap smearing NTP server will cause the leap second to be applied twice. We found this information in Section 5: Using NTP's Leap Second Smearing, from this NTP link: <https://docs.ntpsec.org/latest/leapsmear.html>

We are also concerned with the interaction between the GNSS input reference and NTP input. GNSS (such as the GPS satellites) will announce the leap second pending several months prior to the event, flagging the SecureSync to automatically apply the full leap second on the very last second of the applicable month (June or December).

When smearing the leap second, NTP does not notify of the coming leap second - because it will be applied gradually. If you have some systems using the GNSS synced time (such as PTP outputs, ASCII outputs, etc) and some syncing to the SecureSync via NTP, during the month of the leap second, there absolutely could be a time mismatch between them (with the time mis-match ending after the leap second has been asserted).

As a SecureSync normally syncing via both GNSS and NTP input, we recommend using a NIST NTP server, or the NTP pool servers as an internet time backup, to prevent likely timing issues in the system.

If you have NTP clients you wish to leap smear in the event of another leap second in the future, my recommendation is to temporarily (starting just before the month of the leap second is to be asserted, until after the leap second has been officially asserted) point those NTP clients directly at the Google server, instead of at the SecureSync.

---

## Leap second event for PTP (both the 1204-12 and 1204-32 PTP Option Cards)

- 12 hours prior to the insertion, the Announce message indicates a leap second is pending.
- Because PTP time stamps are in TAI time (which doesn't observe leap seconds), the time stamps at the moment of the leap second are going to count up sequentially just like nothing happened (no two seconds are duplicated like they are in NTP). It's up to the clients to update the UTC to TAI offset value correctly at the

moment of leap second.

**Leap second event for NTP:**

**A) 24 hours prior to leap second is inserted (00:00:00 UTC, the day prior)**

1. LI bits are initially “00”
2. System Time notifies NTP that leap second is pending

**B) ntpq -c as CLI command will change the pps.peer (second row) to “leap\_armed”**

**note:** ntpq rv command also reports leap second info.

```
Every 1.0s: ntpq -c as Tue Jun 30 23:37:31 2015

ind assid status conf reach auth condition last_event cnt
=====
 1  8786  9664  yes  yes  none  sys.peer  reachable  6
 2  8787  9769  yes  yes  none  pps.peer  leap_armed  6
```

**C) LI bits change to “01” in Management -> NTP Setup page of the browser (and in the NTP packets) to 01.**

```
spadmin@Spectracom176:~
Every 2.0s: ntpq -c sysinfo Tue Jun 30 23:50:57 2015

associd=0 status=4118 leap_add_sec, sync_pps, 1 event, no_sys_peer,
system peer: PPS(0)
system peer mode: client
leap indicator: 01
stratum: 1
log2 precision: -18
root delay: 0.000
root dispersion: 1.000
reference ID: PPS
reference time: d93da9e0.d8a2a776 Tue, Jun 30 2015 23:50:56.846
system jitter: 0.030352
clock jitter: 0.008
clock wander: 0.146
broadcast delay: 0.000
symm. auth. delay: 0.000
```

**D) At the leap second insertion (23:59:59 UTC on the day of the leap second being inserted)**

1. NTP should go to “60”
2. The Front panel should display the seconds as “60”.

**E) Just after the leap second insertion. Leap indicator bits go back to “00”**

---

## Associated Log entries for the leap second insertion

### Timing log and System log

- Just the Happy New Year message was inserted for the start of the year.

### 1) When GPS has flagged the system months in advance that a leap second is pending at the end of June or Dec

- When the GPS receiver starts to see a pending leap second being announced in the GPS signal, this is flagged in the **System** log (the example below was from our internal house reference)

|                 |          |                                                                |
|-----------------|----------|----------------------------------------------------------------|
| Jul 19 15:53:46 | [system] | Scheduled Leap Second: +1 sec at 00:00:00 001/2017 UTC (KMOND) |
|-----------------|----------|----------------------------------------------------------------|

“Scheduled leap second: +1 second .”

**Note:** This log entry will only be observed in the System log, later than the date it was asserted, if it hasn't already been rotated out (the System log may need to go back to as much as 6 months in order for it to still be in the logs). But if the logs are being sent to a remote syslog server, it may still be present in the syslog server

**Note:** This next scheduled leap second is also logged in the System log after each subsequent reboot.

### 2) Day of the leap second insertion

**Note:** the Log entries below are from the 31 Dec, 2016 leap second (filtered for “leap”) with v5.5.0 installed and ublox GPS being the selected reference.

### F) Kernel log

Dec 31 23:59:59 Spectracom kernel: Clock: inserting leap second 23:59:60 UTC  
Jan 01 00:00:00 Spectracom Spectracom: [fcron] Happy New Year Sun Jan 1 00:00:00 UTC 2017

### G) NTP log

The **Tools** -> **NTP** log page should have four new log entries associated with leap sec (below in ascending order. Screenshot is in descending order):

1. “...leap\_armed” (about 24 hours prior to the leap second insertion)
2. “kernel reports leap second insertion scheduled” (about 24 hours prior to the leap second insertion)
3. “...leap\_event” (at the moment of the leap occurring)
4. “kernel reports leap second has occurred” ( just a few seconds after the moment of the leap occurring)

| Id   | Date            | Entity       | Message                                        |
|------|-----------------|--------------|------------------------------------------------|
| 2983 | Jan 01 00:00:04 | ntpd[15323]: | kernel reports leap second has occurred        |
| 2982 | Jan 01 00:00:04 | ntpd[15323]: | kernel reports leap second has occurred        |
| 2981 | Jan 01 00:00:00 | ntpd[15323]: | 0.0.0.0 411b 0b leap_event                     |
| 2955 | Dec 31 00:00:21 | ntpd[15323]: | kernel reports leap second insertion scheduled |
| 2954 | Dec 31 00:00:11 | ntpd[15323]: | PPS(0) 9749 89 leap_armed                      |

**Note:** The two “kernel reports leap second has occurred” log entries are at the exact same time and for the exact same event. Having the event logged twice is just a factor of how logging works and not a software defect.

**H) Qual log (no direct log entries for leap second, but the first entry after the insertion should have a Q= value of 3601)**

**Email Keith sent:** Most logs don't have “routine” entries. They only have new entries asserted in them when a particular event happens. But there is one log that needs to account for every second in each hour that the unit is powered-up, the GNSS Qualification log.

The Qual.log reports the total number of satellites being tracked each hour. Since there are normally **3600** seconds in an hour, each qual log entry accounts for 3600 seconds, reported with a “Q=” value at the end of each entry (if the receiver is tracking at least one satellite for the hour. the Q value will normally be 3600.

But if the leap second was added as expected, there will be a total of **3601** seconds in the log entry for 1 Jan 01:00 UTC log entry (the first entry following the leap insertion).

The entry below in red has a Q value of 3601, whereas all other entries before and after have a e value of 3600.

an 01 00:00:00 Spectracom Spectracom: [fcron] Happy New Year Sun Jan 1 00:00:00 UTC 2017  
 Jan 1 00:00:01 Spectracom Spectracom: [system] GPS 0: 8 = 6 9 = 953 10 = 2212 11 = 429 Q = 3600  
 Jan 1 01:00:02 Spectracom Spectracom: [system] GPS 0: 7 = 12 8 = 75 9 = 1060 10 = 1956 11 = 233 12 = 265 Q = 3601  
 Jan 1 02:00:02 Spectracom Spectracom: [system] GPS 0: 7 = 232 8 = 1395 9 = 1762 10 = 211 Q = 3600  
 Jan 1 03:00:02 Spectracom Spectracom: [system] GPS 0: 7 = 32 8 = 139 9 = 1428 10 = 2001 Q = 3600  
 Jan 1 04:00:02 Spectracom Spectracom: [system] GPS 0: 8 = 70 9 = 1975 10 = 1555 Q = 3600  
 Jan 1 05:00:02 Spectracom Spectracom: [system] GPS 0: 8 = 133 9 = 3051 10 = 416 Q = 3600  
 Jan 1 06:00:02 Spectracom Spectracom: [system] GPS 0: 8 = 1217 9 = 174 10 = 1305 11 = 904 Q = 3600  
 Jan 1 07:00:02 Spectracom Spectracom: [system] GPS 0: 9 = 63 10 = 1209 11 = 2168 12 = 160 Q = 3600

If the leap wasn't correctly added, its Q value wouldn't be 3601.

---

## **New IRIG Control field added to distribute leap second info earlier than just one hour**

- Refer to Mantis case 3008.
- Version 5.2.1 Added new IRIG control field format, Spectracom IEEE C37, to extend leap second notification to a month.
- Intended for SecureSyncs syncing via IRIG input and outputting NTP (SecureSync acting like a Slave to another SecureSync). Without this new control field, the leap second won't be announced until just one minute before the leap second is inserted. This doesn't leave enough time for NTP on those IRIG units to read the leap second and announce it in time.
- Was primarily for Verizon, but others can benefit from this new capability

---

## **Observed issues associated with leap second insertion:**

- Leap second 2015: Leap second keeps being asserted at the end of each month (or only at the end of the following July or Dec) after a leap second was scheduled to occur (leap second keeps being inserted)
- Refer to Mantis case 3215
- This issue was observed with two 9300 series customers but can also apply to 9400s/SecureSyncs running earlier versions of NTP (NTP 4.2.6 and below).
- Associated with NTP bug 2246 ("sys\_leap is sticky"): [http://bugs.ntp.org/show\\_bug.cgi?id=2246](http://bugs.ntp.org/show_bug.cgi?id=2246)
- Search for "NTP bug 2246" in Custserviceassistance and/or NetClock customer assistance documents for more details on this potential condition.

### **Leap second 2015: Skylight Version 4.7L didn't change the LI bits from 00 to 01 within 24 hours of the leap second being inserted**

- Refer to Salesforce case 18412.
- Leap second was properly scheduled by GPS. But the LI bits hadn't changed from 00 to 01 within 24 hours of the leap second (as verified about 8 hours prior to the leap second).
- Recommended manually changing the UTC offset value from 16 to 17 in the *Setup -> Time Management* page of the browser at the moment of the leap second being applied.

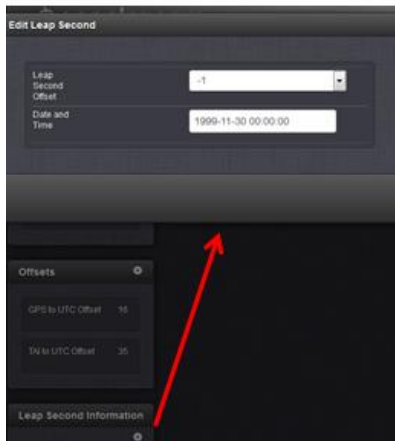
## **Issue with Leap Second not being able to be "removed" after scheduling**

- Versions 5.2.0 and below: after scheduling a leap second, can reschedule another leap second, but can't completely clear the schedule.
- Refer to Mantis Case 3027: Added ability to delete leap second in version 5.2.1 release (May 2015).

## **Web browser interface pages associated with leap second**

### **I) Newer web browser (versions 5.1.2 and above)**

**Management -> Time Management** page (bottom-left corner)



## J) Classic interface browser

System -> System Time page

**System Time:**

Set System Time using user-specified UTC time below

Date: 6 Jan 2015

Time: 22 : 38 : 43

**Leap Seconds:**

Number of leap seconds between UTC and GPS time: 16

### CLI command for reading the next scheduled leap second

- Command to get the next scheduled leap second: **CS\_GetLeapSec 0**

```
spadmin@CustService-177 ~ $ CS_GetLeapSec 0
Leap Second: +0 sec at 00:00:00 000/0000 UTC
spadmin@CustService-177 ~ $
```

**Note:** User doesn't have permission to schedule the next leap second via the cli. It needs to be scheduled via the browser.

```
spadmin@CustService-177 ~ $ CS_SetLeapSec 0
-bash: /usr/bin/CS_SetLeapSec: Permission denied
spadmin@CustService-177 ~ $ CS_SetLeapSec 0
```

- I wanted to make sure that leap seconds events information is automatically passed down to Stratum-3 clients.

**Reply from Sam Otto (2 Apr 2013) which was reviewed by Dave Sohn:** Correct, The Stratum-2 does pass along the leap second bits 24 hours prior to the leap second event.

#### Email from Paul Myers (15 Feb 2013)

The scheduled leap second will tell the KTS clock to make a leap second adjustment.

The KTS will be read by the network processor using the NTP Reference Clock driver.

The NTP daemon will be aware of a pending leap second and will schedule one in the Linux kernel.



There will be a single leap second inserted by the KTS, received on the 60<sup>th</sup> second of the havequick input, and the NTP and linux kernel will be aware of only a single leap second.

There is not issue with 2 leap seconds, being adjusted.

The NTP step should occur at or be logged shortly after the leap second. I do agree I have seen the step logged slightly late before, but I can't remember under which circumstance of testing. If it was a unscheduled leap second or a scheduled one...

To ensure your customer is satisfied I recommend you have someone perform this test:

1. Handset the time to several hours before a leap second adjustment on 2 SecureSyncs and let them sync the linux time to NTP
2. Using a SecureSync with HaveQuick output schedule a leap second using the format without notification
3. Sync SecureSync with a havequick input card
4. Ensure NTP is synced and the time is set correctly.
5. Hand set a scheduled leap second several hours hence
6. Allow the NTP to sync
7. Verify the LI bits indicate a leap second is pending
8. Configure the Front Panel, ASCII output, etc so you can watch the leap second rollover
9. Observe the rollover
  - You will observe the 58, 59, 60, 0, 1, 2
  - You will observe a 1 second step in the NTP log slightly after the rollover
  - This is normal behavior.
  - KTS, Linux and NTP are all aware of the 60<sup>th</sup> second.
  - NTP will distribute the scheduled leap second by sending leap indicator LI bits set to other NTP servers.

**From:** Paul Myers

**Subject:** Leap Second Document

<\\Roc.spectracom.us\CS\Engineering\Projects\Lafayette\301 Verification Test Results\Release 4.8.2\Leap Second Changes.docx>

This is my first cut at the leap second document. I will improve it where it is not clear or additions are needed.

In general what was done was:

- Improve Clock Service to better handle leap seconds when operating in Time Scales other than UTC and provide functions to facilitate time scale conversions
- Time Manipulation library
- Output 60 for the leap second when appropriate
- Fix Time conversions so errors don't happen
- Fix NTP stratum 2 to avoid premature leap second announcers.
- Fix Leap Indicators in any Outputs that were not working
- Detect leap seconds as appropriate in any Input References that did not.
- Fix any error conditions found
- Implement and test HaveQuick Leap Seconds

The document above contains a list of all files changed since 4.8.0 to NOW (pre-4.8.3) which were changed for Leap Second related reasons.

Also, it contains at the end information for Keith to write Leap Second Application note as to what features are improved and why.

I think Keith should read it, if it is not clear enough tell me, and I can fix it, and then he can shorten it to say if you are using ASCII and you need this update. If you don't you may have this problem such as skipped Leap Second, late adjustment, no 60 values, wrong GPS-UTC offset briefly, etc.

I will likely update it with any of Mark's changes and any feedback he has.

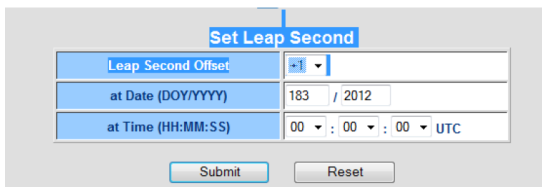
Email from Paul Myers about manually scheduling a leap second (14 Feb 2013)  
I believe the manual is incorrect about scheduling leap seconds.

Mark Goodlein designed the interface to set Leap Seconds in both the SecureSync and in the KTS.

The time to 'schedule' them was 1 second after the adjustment. In theory they can be added or removed.

The constant is the time after.

I ran the GSG Leap Second test and observed what was 'scheduled' in KTS.



| Set Leap Second                                                            |                  |
|----------------------------------------------------------------------------|------------------|
| Leap Second Offset                                                         | +1               |
| at Date (DOY/YYYY)                                                         | 183 / 2012       |
| at Time (HH:MM:SS)                                                         | 00 : 00 : 00 UTC |
| <input type="button" value="Submit"/> <input type="button" value="Reset"/> |                  |

Note that for a +1 adjustment at 23:59:59 on 182/2012 the above scheduled date is shown.

To similarly schedule a leap second you must do the same. SO the 23:59:59 in the manual is incorrect in my opinion.

**Note:** when testing Leap Second functionality, make sure no external references are connected/present. If a user manually sets a leap second with a reference connected, the reference will interfere with the test results, and may cause abnormal output time stamps!

**Email from Paul Myers:**

To simulate a Leap Second Rollover you CANNOT have a reference attached as it will try to correct the time if you handset a leap second that is NOT provided by a Reference.

**To handset a leap second condition:**

1. Remove all references.
2. Handset the clock to the desired time say 23:58:00 hours, Day 366 of a leap year or 365 of a non-leap year
3. Handset the rollover to the first second of the next day. 1/year 00:00:00
4. Watch the rollover condition

---

**Note:** Responses to questions below are from **Paul Myers**

- To confirm, if an input reference doesn't provide Leap Second pending notification (such as not using extended havequick) , a user can still manually schedule a pending leap second via the "Set Leap Second" section of the Setup- > Time Management page? Manually scheduling the leap second should result in System Time making a one second time jump at the last second of the scheduled month.

**[PEM]** The user can schedule a leap second when a reference is present or not.

**[PEM]** The leap second gets automatically updated if the reference is aware of leap seconds.

**[PEM]** NTP will be made aware leap seconds from the Reference clock driver or in the case of NTP Stratum 2-15 servers from NTP packets LI bits.

- If the leap second section is filled in by a user (because the input reference can't set these fields), will NTP know to apply a one second jump correction at the last second of the scheduled month? Or, as I suspect, will NTP instead slew its time by one second, once System Time makes the one second time jump at the last second of the month).

[PEM] Yes. NTP will be informed of the pending leap second because the reference clock driver communicates this information along with time to the NTP from the KTS. NTP will make its leap second adjustment 58, 59, 60, 0, 1, by adjusting the kernel time. NTP can step the second and slew in the remainder. If NTP is NOT notified of the pending leap second it will have to step/slew to correct the offset later based upon poll rate. NTP sets its LI bits to indicate a leap second is pending 24 hours before the leap second insertion.

- If NTP slews its time for the one second time jump that occurs in System Time, over how long of a period will NTP need to slew the time until its correct again? Does the current poll interval affect how long it takes to slew its time by one second?

[PEM] It depends up on poll rate, but scheduled leap seconds are known to the kernel and NTP to be handled. Unplanned offsets can take longer.

---

## LI Bits (Leap indicator bits) now displayed in the *Status -> NTP* page of the browser

Starting in version 4.8.4, the LI bits were added to the NTP input references tables. Earlier versions of software did not display the LI bits in each row of the tables.

Leap second testing only allows leap second to occur last day of June or last day of December  
Paul Myers coded the Leap Second functionality to allow Leap Second to only be able to occur on the last day of June or December. When testing for Leap second, set the leap second to occur on one of these two days only. Then with User mode enabled, manually set the date/time for a day prior to leap second, to see it occur.

---

## NetClock 9400/SecureSync that is synced via NTP

The following is from <http://www.meinberg.de/english/info/leap-second.htm#irig>:

IRIG time codes are often used to synchronize time between computers and other devices via cables or fiber optic connections.

Several IRIG frame types have been specified to transport time information between two IRIG devices. Most of the commonly used IRIG frames carry the day-of-year and the current time, but they do neither contain the year number which would be required to convert the day-of-year to a calendar date unambiguously in leap years and non-leap years, nor the UTC offset of the transported time, or a leap second announcement.

The IRIG frame type **IEEE1344** contains all this information. However, by specification the leap second is announced only about 60 seconds before it actually occurs.

If such an IRIG receiver is used as a reference time source for NTP then there's a good chance the NTP daemon misses the leap second announcement at a polling interval of 64 seconds and thus is unable to handle the leap second correctly. Even if the NTP daemon received the leap second announcement, it was too late to pass the announcement on to the clients, so most of the NTP clients would probably miss the leap second.

This is the reason why in general a leap second file should be installed for NTP if an IRIG receiver is used as reference time source.

If the NTP server that SecureSync is synced to is synced via IRIG, as IRIG only changed the LI bits one minute before the leap second occurs, will require NTP to step the time about 15-20 minutes thereafter, to account for the one second time change.

**Email from Keith to Rob Amos (ASX) 7/13/12**

Hi Rob,

Good day to you!

We have reviewed the SecureSync logs you sent to us (thanks for sending them to us)!! I have some feedback for you that should help!

To begin, attached are individual documents for each SecureSync, with each document excerpting the log entries relating to the leap second time-frame. At the end of each document is a list of our findings, for that particular SecureSync.

In short summary of all of the logs, the SecureSyncs properly handled the leap second insertion. However, we fell "victim" to the

IRIG reference not providing enough advance warning of the pending leap second. Because only one minute of advanced warning was provided to the kernel, the leap second time correction was delayed by several minutes after the leap second insertion occurred.

### Now for the details:

First: two points for clarification:

- NTP adjusts the SecureSync's kernel "Time" by one second for the leap second insertion.
- The System Time's (displayed in the Time Management page of the browser) leap second flag adjusts the Timing System's time scale offsets (such as the UTC to TAI offset, as needed for PTP) by one second when the leap second insertion has occurred.

The SecureSync's System time for its outputs is derived from the kernel time, which is updated by NTP and its selected reference. NTP can select various input references to synchronize with (such as GPS or NTP, for examples). When NTP is synced to GPS (via the System Time) NTP has a direct and continuous time reference to sync with. However, when NTP is syncing to another NTP time server, the time stamps to sync NTP with are only periodically available (with the interval based on the poll rate of its selected NTP server (as determined by NTP, to be between the configured MinPoll and MaxPoll intervals).

Even though the Stratum 1 server only gave one minute of advanced notice of the pending leap second, we were fortunate that the SecureSync had been able to sync to GPS at least once since March. When the SecureSync synced to GPS, it flagged the system to the pending leap second, well in advance. If it hadn't been for this GPS selection, the only way SecureSync would have known to update its time offset corrections (such as the TAI offset) at the moment of the leap second is if NTP had been provided ample notice to the pending leap second. Since GPS had already flagged the leap second prior to the leap second, SecureSync was able to correct the offsets just after the leap second was asserted.

In addition to the System Time offset for TAI needing to be updated at the leap second, the System time (kernel time) also needed to be updated by one second, as well. NTP updates the kernel (which is the time reference for the system) for this one second correction. As long as NTP can obtain from its selected reference, sufficient notice of the pending leap second before it actually occurs, the kernel time is automatically corrected at the correct second. However, if NTP cannot obtain sufficient advanced notice from its selected reference before it's inserted, the time correction is delayed until it can receive the LI bit change from its reference.

The PTP Option Cards, when configured as a PTP Master, read the System time every second. So once both the UTC to TAI offset as well as the kernel time have been corrected by one second, the PTP Master sends out the corrected time, immediately thereafter.

Specific to the logs you sent:

The logs you sent show that the System's time correction (the kernel "step") occurred on all of the SecureSyncs between 15:29 and 19:53 (Minutes / Seconds) after the leap second had been inserted. This is because this was the first opportunity it had to obtain the LI bit change from its selected NTP reference and to apply the leap second to the kernel time.

If the SecureSyncs had been synced to GPS prior the leap second insertion (instead of to the Stratum 1 NTP server) the SecureSync's time would have adjusted at 23:59:60 two to three seconds after the leap second was inserted, instead of 15 to 20 minutes thereafter (as a result of the poll interval for the Stratum 1 server).

For any future leap second that may occur, we initially discussed potentially having you change both the Min and Max Poll intervals for the Stratum 1 server configuration to "4 (16 seconds)" on the day of the leap second. This would ensure NTP polled the Stratum 1 server every 16 second and therefore a couple of times during the one minute period that the Stratum 1 server has the LI bits set to indicate the pending leap second. However, we tested this and found that only one minute of advanced notice from the NTP reference, even at the quickest possible NTP poll interval, does not provide enough advanced notice to the kernel to apply the time correction at the leap second. Because the kernel was not able to flagged to correct the time at the Leap second, when the selected input is another NTP server, a few polls after the leap second occurred, NTP realized a one second step was needed. So about 15 to 20 minutes later, NTP stepped the kernel time on your SecureSyncs (other SecureSyncs using input references such

as GPS, did not need to step the kernel after the leap second- the time was automatically corrected at the correct second because the kernel had ample notice of the pending leap second).

**In summary of the above information:**

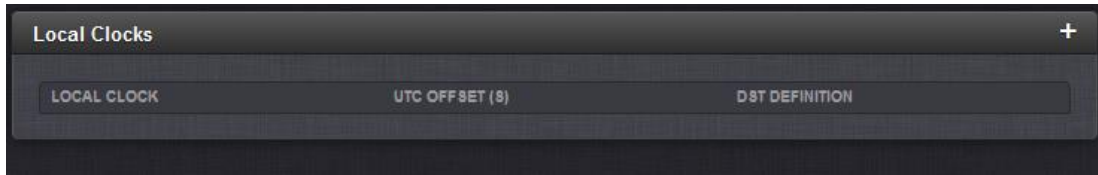
The GPS input had flagged the timing system of the pending leap second, well in advance (GPS started broadcasting this information on the leap second back in the March time-frame) this allowed the timing system to adjust the TAI offset within just a couple of seconds of the leap second. However, the IRIG signal limiting the LI bit change to only one minute did not provide the kernel with enough advanced notice.

So, our recommendation to you, if another leap second is scheduled in the future (and since it's unlikely that the IRIG reference can provide a longer advanced notice with the LI bit change occurring earlier than just one minute prior), would be to temporarily select GPS as the highest priority reference (instead of NTP) on the day of the leap second, via the Reference Priority table. This will provide both NTP and the timing system with sufficient advanced notice to prevent the need for NTP to have to step the time several minutes after the leap second has been inserted. Then, switch back to using NTP as the selected reference by making it the highest priority reference. Otherwise, using NTP as the input during the leap second will result in a delay of the one second time correction of the NTP and PTP timing outputs.

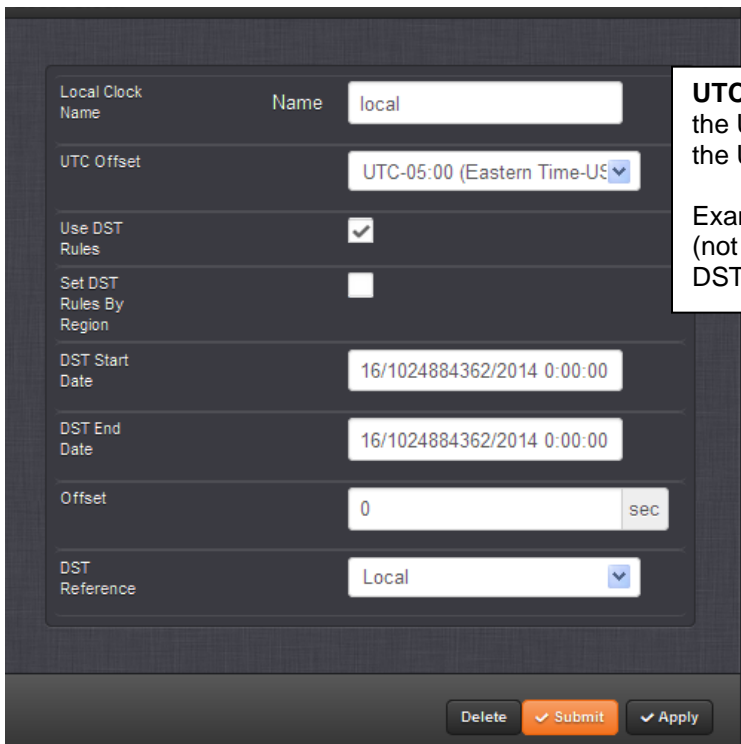
## \*\*Local System Clocks (Local Clock)

New web browser (version 5.1.2 and above)

*Management* -> *Time Management* (click on the + to add a new local clock)



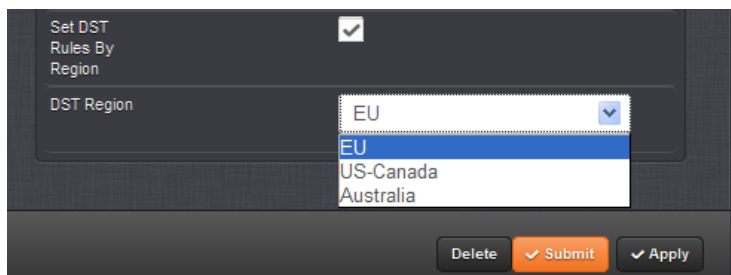
If "Use DST rules" is selected, bottom of page expands.



**UTC Offset:** Always set this drop-down to the UTC offset during **STANDARD** time (not the UTC offset during **DST** time)

Example for **Australia**, set to UTC +10:00 (not UTC +11:00 which is their offset during DST)

Select "Set DST Rules by Region" select region, and then Submit or Apply.



## DST Configuration

- Local clock configuration is stored in the "drdf.conf" file (**/config** directory) Example entry below:

```

spadmin@Spectracom ~/config $ cat drdf.conf
U 1 3 5 0 1 10 5 0 1 3600
S-Canada 0 3 2 0 2 11 1 0 2 3600
Australia 0 10 1 0 2 4 1 0 3 3600

```

To view all created local system clocks in the SecureSync config file:

- 1) telnet/ssh into the unit.
- 2) Type: **cd config** (to go to the home/spectracom/config directory)
- 3) type **cat lcdf.conf**

Should respond with no response (back to the command prompt) if no local clocks have been created. Or, one line of configurations for each local clock that has been created.

Typical responses after creating/deleting clocks

```

[spadmin@Spectracom ~]$ cd config
[spadmin@Spectracom config]$ cat lcdf.conf
Sheriff 0 -21600 0 3 2 0 2 11 1 0 2 3600
sheriff2 0 -21600 0 3 2 0 2 11 1 0 2 3600
[spadmin@Spectracom config]$ cat lcdf.conf
[spadmin@Spectracom config]$ cat lcdf.conf
Central 0 -21600 0 3 2 0 2 11 1 0 2 3600
[spadmin@Spectracom config]$

```

## Local Clock rules in a mobile environment

### Time Zone Setup Section

#### Time Zone Definition field set to “Automatically configure to unit’s physical locality”

(At least version 5.0.0 and prior) This config is NOT dynamic. It uses a single instance of GPS position to configure the Time Zone Offset for where it’s located WHEN THE LOCAL CLOCK WAS CONFIGURED. It does not update Time Zone Offset if the equipment is physically moved into another Time Zone.

A feature Mantis case is being submitted per a request from Donald Harris to have it update per its current GPS coordinates.

**Email from Dave Lorah to Donald Harris:** Yes, that is correct. The Local Clock setting will need to be setup at each individual site by using the Automatically Configured mode or manually selected time zone. This is only for the Local Clock settings. The Garmin is designed for that. The SecureSync is 99.99% of the time used in stationary environments so this is usually not a problem.

I am afraid this is our only option.

We could consider this as a feature enhancement, but I’d caution that the automatic time zone detection is not foolproof. It is based on longitudinal lines, which don’t necessarily line up nicely all the time with time zones.

#### Modified email from Dick Fox to TOYO (3/13/12)

The short answer is No we can’t automatically update the local clock time zone offset based on GPS location and send out a local IRIG code that reflects the local time zone based on dynamic position.

Here are the details:

1. IRIG can send out a time code based on a local clock
2. On initial Setup, SecureSync can use the GPS position to setup a time zone offset used for a local clock
3. However, SecureSync’s GPS position is only used for initial setup of the local clock. As the ship moves and the GPS position changes, the time zone is NOT automatically updated based on position.

So if the NTP server moves to a new time zone, the offset would have to be manually changed.

## Known issues with Local Clocks

### A) When a local clock is selected, the RS-485 and RS-232 ports output time adjusts to UTC (+8 seconds) offset

Refer to Mantis case 2760 <http://cvsmantis.int.oroila.com/mantis/view.php?id=2760>

Started in version 5.1.2 - Fixed in version 5.2.0.

I have entered NC 7724 as a Yellow NC for a 5.1.2 bug:

SecureSync 5.1.2 new web browser will not properly configure the Local Clock setting for the 9483 RS-232 and RS-485 ports. When a local clock is configured to these ports the time adjusts to UTC+ 8 seconds offset. After configuring the local clock setting to the RS-232 port in the new web browser, when switching to the Classic Interface the TimeScale field is selected as "Local" but there is no entry in the Local Clock field.

I have duplicated this in the 9483 RS-232 and RS-485 interfaces. Not sure how many other option cards this affects.

Should not need a "stop shipment" since the classic interface allows the local clock to be correctly entered.

I entered this in Mantis 0002760.

### B) Changes to a Local clock after it's been applied to inputs/outputs (such as front panel) causes it to be no longer applied to the inputs/outputs. Has to then be re-applied.

- This issue was fixed in version 5.2.1 software update (May 2015)

### C) Empty "DST Region" field drop-down list in the newer (black/charcoal) browser (DST Start and End dates also have erroneous info in them).

The screenshot shows a configuration panel for a local clock. It includes the following fields and controls:

- Local Clock Name:** A text input field containing the value "test".
- UTC Offset:** A dropdown menu currently showing "UTC-05:00 (Eastern Time-US)".
- Use DST Rules:** A checked checkbox.
- Set DST Rules By Region:** A checked checkbox.
- DST Region:** A dropdown menu that is currently empty.

- Refer to Salesforce case 18044
- Engineering suspected issue with MySQL database.

**Email from Dave Lorah (27 May 15)** We think you may be able to save your configuration, then perform the CLEAN operation and then restore the configuration to resolve the error. If we could get the logs from this unit, we could tell more about what happened.

If you could Save and Download the logs and send them to me I will pass them along to the software engineers for evaluation. They can then recommend how best to proceed.

To get the logs go to the web browser and navigate to the Management/Log Configuration page. Then select the "Save and Download All Logs" in the Actions block. This will bundle up the logs so they can be attached to email. Please send these logs if you can.

### D) Super-set Local Clock names (refer to Salesforce Case 5929 for NASA)

At least versions 4.8.6 and below will have issues with Local Clock names that are a super-set of another case-sensitive Local Clock name (Such as "Tom" and "Tom1"). Tom1 is selected as the Local Clock, "Tom" is actually



the Local Clock selected.

Starting in v4.8.6, the pre-defined local clocks names of GPS, TAI and UTC, in the Front Panel setup were moved to the Local Clock selection (Time Scale field was removed). If a Local Clock name is created with any of these same case-sensitive letters, (such as "UTC-NONE"), and this name is selected in the drop-down, after hitting Submit, "UTC" is actually displayed/selected in the "Local Clock" field.

**In summary:**

- The only letters that can't be capital letters in the Local Clock name are the ones at the beginning of the name that happen to match the default names in the "Local Clock" drop-down (UTC, TAI and GPS).
- Each Local Clock that is created shouldn't be a super-set of another Local Clock name that has already been created (with the same case-sensitive letters). For example, if you have one named "Eastern", you shouldn't create another one call "Eastern-DST". Otherwise, if you try to select "Eastern-DST", "Eastern" will actually be selected.

## Input references / Reference Priority table/ Reference Monitor/Time Sync / Holdover

\*Input References (GPS-GNSS/Glonass/SAASM, PTP, IRIG, Freq in NTP, Havequick, ASCII, etc) /Reference Priority table/Time to synchronize to input reference

### Input Reference designations for SecureSync (as of 6/5/12)

| Reference Designation                    | CLI "Status" command displays | Input description                                       | Refer to Hyperlink Section below                         |
|------------------------------------------|-------------------------------|---------------------------------------------------------|----------------------------------------------------------|
| GPS/GNSS                                 | gps                           | GPS / Glonass<br>(SAASM GPS)                            | <a href="#">GPS/Glonass</a><br><a href="#">SAASM GPS</a> |
| IRIG                                     | ir                            | IRIG (Inter-Range Instrumentation Group)                | <a href="#">IRIG</a>                                     |
| HaveQuick                                | hvq                           | HaveQuick/Stanag                                        | <a href="#">HaveQuick</a>                                |
| ASCII Timecode                           | asc                           | ASCII time code reference                               | <a href="#">ASCII</a>                                    |
| Local System                             | self                          | SecureSync's built-in clock OR internal 1PPS generation | <a href="#">Local System</a>                             |
| NTP                                      | hst1                          | NTP (Network Time Protocol)                             | <a href="#">NTP</a>                                      |
| PTP                                      | ptp                           | PTP (Precision Time Protocol)                           | <a href="#">PTP</a>                                      |
| User                                     | User                          | Manually set time/Battery backed time                   | <a href="#">User/User</a>                                |
| External 1PPS                            | epp                           | External 1PPS reference                                 | <a href="#">EPP0</a>                                     |
| Frequency in (such as 1kHz to 10 MHz in) | frq                           | Frequency Reference                                     | <a href="#">Frequency input (such as 10 MHz)</a>         |
| 10 MHz/T1/E1                             | N/A                           | /T1/E1 from an external source                          | <a href="#">T1 and E1 input</a>                          |

Note that some of these will be followed by a number (such as GPS 0 or IRIG 0). This number can vary, based on the number of similar inputs. GPS is currently limited to just one instance, so this one is currently always GPS 0. However, there can be multiple instances of the same inputs, such as IRIG. So this number may not always be a 0.

### Input "Reference Priority" table

**Note:** The Reference Priority table settings are stored in the *rmnf.conf* file (located in the */config* directory)

### CLI commands used to configure the Reference Priority table

```
spadmin@Spectracom176 ~ $ stateset
Invalid arguments
Usage: stateset <index> <state>
index: 0..15
state: 0=disable, 1=enable
```

- To display the Reference Priority table: **reftable** <enter>
- To enable/disable entries in the Reference Priority table: **stateset** <enter>
- To set the priority of an entry in the Reference Priority table: **priorset** <enter>

**A) Via newer browser (Archive versions 5.1.2 and higher)**  
**Management -> Reference Priority page**

| Priority | Time   | 1PPS   | Enabled                             | Action |
|----------|--------|--------|-------------------------------------|--------|
| 1        | GNSS 0 | GNSS 0 | <input checked="" type="checkbox"/> | Delete |
| 2        | PTP 0  | PTP 0  | <input checked="" type="checkbox"/> | Delete |
| 3        | NTP 1  | NTP 1  | <input checked="" type="checkbox"/> | Delete |
| 4        | User 0 | User 0 | <input checked="" type="checkbox"/> | Delete |

Reset Submit

**B) Via Classic interface browser**

## \*\*Input Reference Monitoring (5.4.5 and above)

- Link to Reference Monitor info in SecureSync online manual:  
[http://manuals.spectracom.com/TS/Content/TS/Topics/ToO\\_InpRefs.htm?Highlight=reference%20monitor](http://manuals.spectracom.com/TS/Content/TS/Topics/ToO_InpRefs.htm?Highlight=reference%20monitor)

Note that if you click on the figures in this guide, they will expand and become much clearer!!

- Allows comparison of filtered phase offsets between input references (Individually compares each reference against the System's on-time point)
- The phase values shown are the filtered phase differences between each input reference 1PPS, and the internal disciplined 1PPS.

## REFERENCE QUALITY MONITORING

Add infrastructure to timing system to measure performance of non-synchronizing references

Phase error

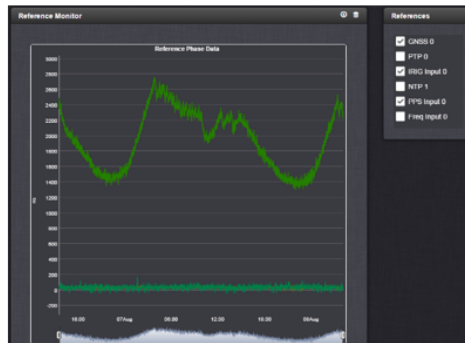
- Measured against current system state (phase error against current system 1PPS)

Initially provide graphical measurements similar to current disciplining graphs with inputs overlaid

- Expand to provide additional statistical information in relation to system state and other references

Add additional functionality using infrastructure

- Add quality bands to reference source selection
- Add multiple reference disciplining
- Add spoofing detection / alarming based on additional references

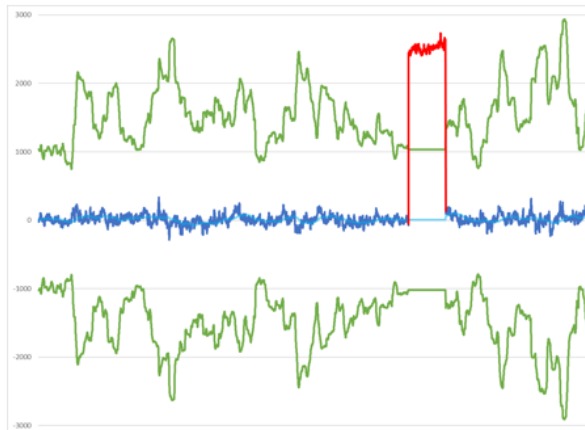


## SINGLE REFERENCE QUALIFICATION

Phase and frequency validation is done per reference against the internal oscillator

- Phase Validity Monitoring
- Running long term averages and standard deviations are calculated to generate validity thresholds
- Live phase measurements are checked against these thresholds to catch short term phase drift and jumps
- Jan 2016 13 usec GPS glitch
- Frequency Validity Monitoring
- Oscillator characteristics (aging, temperature stability) are used to generate frequency thresholds taking into account oscillator temperature measurements
- Frequency measurements of monitored references are validated against these thresholds
- Oscillator control history is also validated using these thresholds

Error detection algorithms like BroadShield are also incorporated into individual reference validation

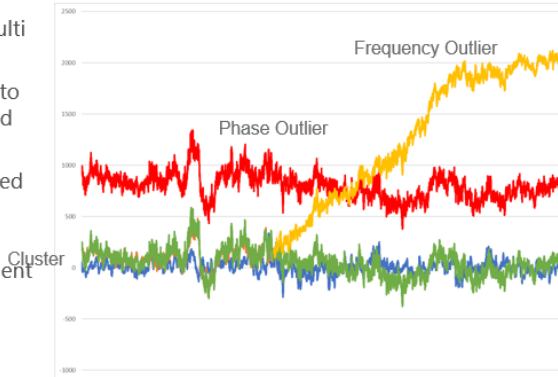


## MULTI REFERENCE QUALIFICATION

References validated by single reference checks are utilized in multi reference qualification checks

- Clustering techniques are used to group references together based on phase/frequency statistics
- Outliers can be determined based on phase biases or frequency drifts

All input references and independent monitoring sources like the fiber optic reference can be utilized in these techniques



---

### Software update changes associated with Reference Monitor

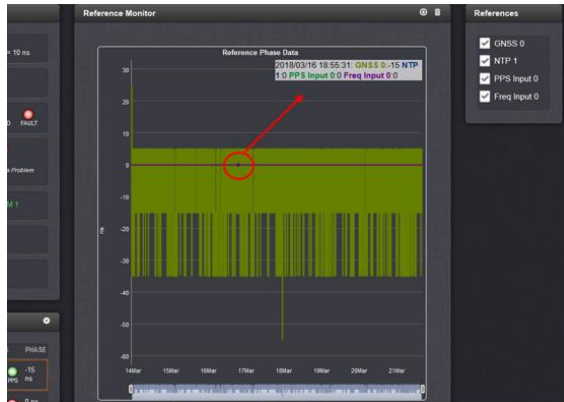
#### A) Version 5.7.0

- 1.Changed the graph data from filtered to unfiltered data (graph is now a bit more “sharp/crisp”)
- 2.Added Smart reference validation/verification. based on phase error data for each reference (details on next page):

#### B) Version 5.4.5

- **Version 5.4.5** added enhanced Reference Quality Monitor status to display record all the available input reference phase errors in the same graph and log file.
  - Data is only displayed in v5.4.5- not used for validation until v5.7.0 (which added smart phase monitor validation)
  - **Version 5.4.5** also added a new .csv file (LogRefMonStatus.csv) to log the selected reference and phase errors

## Tools -> Reference Monitor page of the browser



**Email from Keith (21 Mar 18)** The table on the right of the plot lists all available 1PPS input references, allowing the ability to enable/disable the display of each one in the graph. Mouse-hovering over the graph plot (shown with the red circle I added to the plot) opens a gray display window (upper-right corner of the plot window) displaying the details of each reference at that particular date/time (in UTC timescale) and also indicates the corresponding line color of each reference being displayed in the plot area. The 1PPS phase error on the left side of the plot area, for the actual values of the 1PPS phase error for each input reference, is in "Nanoseconds"

The phase in the Reference Status location is the difference between the Reference and the On-time point (1PPS). So, all the references compare themselves to the System's on-time point.

Reference Monitoring helps to understand and predict system behavior, and is an interference mitigation tool. It can also be used to manually re-organize reference priorities e.g., by assigning a lower reference priority to a noisy reference or a reference with a significant phase offset, or to automatically failover to a different reference if certain quality thresholds are no longer met (see [Smart Reference Monitoring](#)).

SecureSync allows Reference Monitoring by comparing the phase data of references against the System Ontime Point. The phase values shown are the filtered phase differences between each input reference 1PPS, and the internal disciplined 1PPS.

The data is plotted in a graph in real-time. The plot also allows you to display historic data, zoom in on any data range or on a specific reference. A data set can be exported, or deleted.

### To monitor the quality of references:

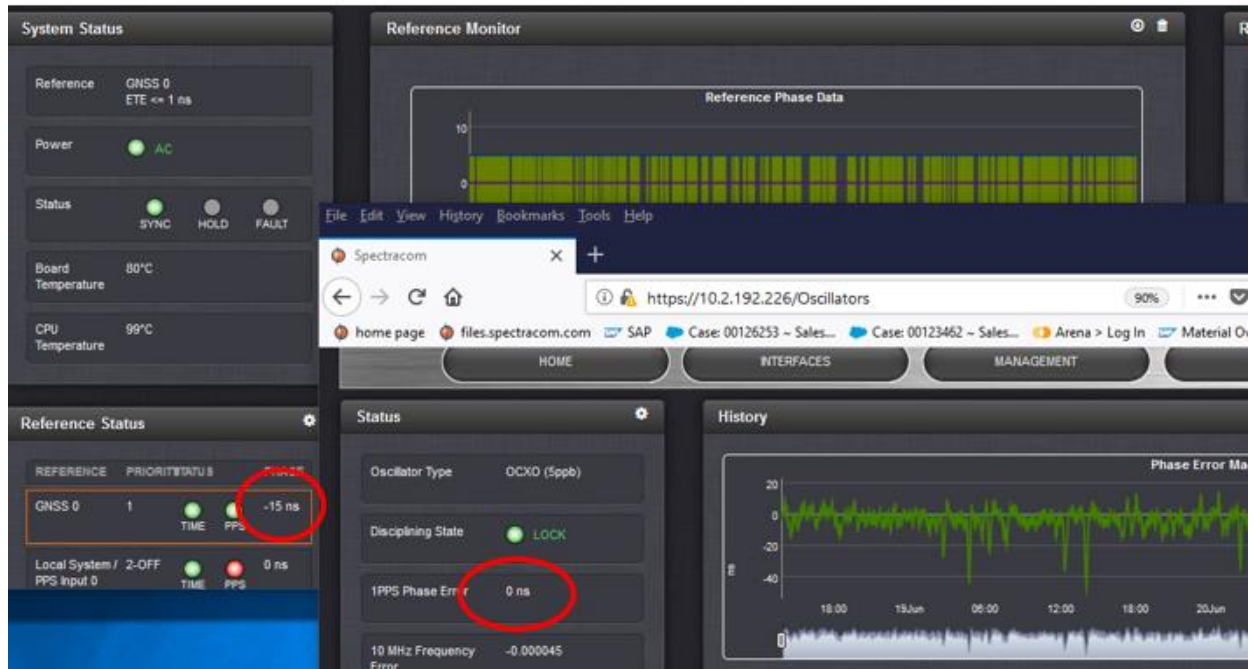
On the left side of the screen, Status information is displayed for the System and the References. Note that the Reference Status panel also displays the latest PHASE OFFSET reading (1) for active references against the System Ontime Point. The reading is updated every 30 seconds.

This Reference Phase Offset Data is plotted over time (abscissa) in the Reference Monitor panel in the center of the screen. Use the check boxes in the References panel (2) to select the reference(s) for which you want to plot the phase offset data. Use the handles (3) to zoom in on a time window.

The scale of the axis of ordinate (4) is determined by the largest amplitude of any of the references displayed in the current time window. Use the checkboxes in the References panel on the right to remove references from the graph, or add them to it

“Side-by-side” variances between “disciplining” phase error values (reported in the *Management -> Disciplining* and *Reference Priority* pages) versus the phase error values reported in the *Tools -> Reference Monitor* page

- Due to differences in granularity in the *Disciplining / Reference Priority* pages, versus the *Reference Monitor* page, the phase error values for the same reference may be reported as two different values.
  - As shown below, the phase error is reported as **0 ns** in the Disciplining page, while the GPS phase error is being reported as **-15 ns** in the Reference Monitor page.



**Per Dave S (19 Jun 2018)** I don't remember the direction of the offset (negative vs positive), but as far as the differences, the disciplining phase error is a filtered error, that has higher resolution. The reference monitor phase errors are raw offset values with a 20ns resolution. They should absolutely track each other in terms of trends, but due to the filtering and differences in resolution/granularity there will be differences in the reported offsets.

**Reference Monitor data logging/storage/deleting (errors may occur when downloading large amounts of data)**

- Data is only written to the sqlite database each minute (at 30 seconds into each minute, such as at 12:01:30, 12:02:30, 12:03:30, etc)
- Data is stored in the "log\_ref\_mon\_statuses" table of the SQLite database
- This data can be cleared out using the **clearstats**<enter> CLI command
  - As data is only placed in the database each minute (at 30 seconds into each minute, such as 12:01:30, 12:02:30, etc) it may be up to one minute after performing clearstats before the database is no longer empty.

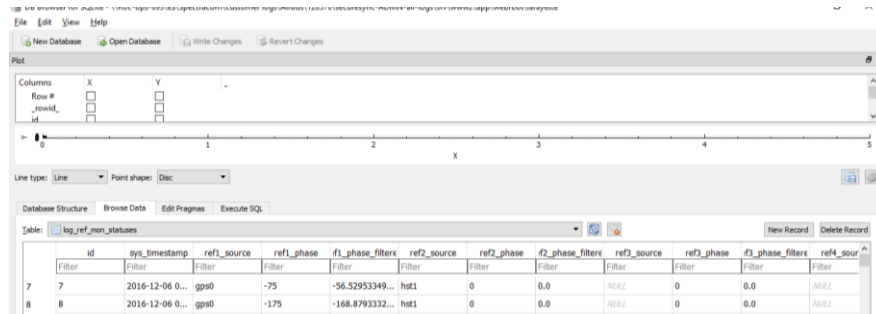
**Exporting the Reference Monitor table data**

➤ This data can be exported from the unit by either:

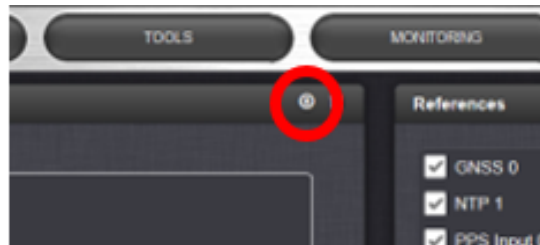
## 1. Saving/exporting the logs:

A. View the **Lafayette** (sqlite) database using the “**DB browser for SQLite.exe**” freeware.

B. In the “**Browse Data**” tab, select the “**log\_red\_mon\_statuses**” table:



2. Or as a .csv file, by clicking the “down arrow” (download) icon (next to the garbage can icon) in the **Tools -> Reference Monitor** page of the browser.



**Note the amount of data in the Reference Monitor table may be too large to be able to use the “download to csv file” button in the browser**

- The csv file download button uses the web browser differently than the log bundle download function to download and convert the sqlite data to a csv file. this download button may not be able to download/convert larger amounts of data.
  - Try unselecting at least some (of not all but one) Reference checkbox on the right-side of the page, which can significantly reduce the amount of data needing to be downloaded/converted to the .csv file

➤ Refer to Salesforce Case 1777373 (Oct 2018, with v5.8.2)

**Attempted download from 'Reference Monitor':**

**<https://<servername>/Logs/getGraphStatus/LogRefMonStatus.csv>  
returns HTTP ERROR 500**

➤ This data can be cleared using the **clearstats**<enter> CLI command

- As data is only placed in the database each minute (at 30 seconds into each minute (such as 12:01:30, 12:02:30, etc) it may be up to one minute after performing clearstats before the database is no longer empty.

**Response from Keith (21 Nov 2018)** I just spoke with the Engineer again and believe we have the explanation for you. Shortly after initially reading your report, he (and then I, after he mentioned it) believed the only issue with the downloading of the table (using the download button in the browser) was strictly related to the amount of data being downloaded via the browser, and also being converted to a csv file. This was also helped confirmed when I initially saw similar conditions occur, until I disabled all but one of the References on the side of the table (so that the data for just one reference was to be downloaded). This resulted in a successful download of this reference's data using the download icon in the browser.



To confirm what you are seeing when downloading the table via the browser icon is a limitation of the amount of data which can be processed by the web browser, please first perform the CLI command of **clearstats**<enter>. This command will only delete the "statistics" data from the database (it doesn't delete any logs, which uses a separate command for these items to be deleted). Very shortly thereafter, perform the download table using the icon in the web browser again, to confirm the data is downloaded/processed successfully, and as expected, into a csv file by the web browser's functionality.

Note that if you wish to download the entire table (instead of selecting various references from the table to individually download data) when there is more extensive data present in this table, note this table is also contained in each Logs bundle file you download from the unit. So, there is a second available method to obtain all the data, besides using the browser download icon (the download icon in the browser uses a different method to download the data to your computer than the logs download function).

The logs bundle (once extracted a couple times to unbundle it) contains the sqlite database, which stores data such as the Monitor table, is housed in the main "srv" folder of the extracted log bundle (there are a couple sub-folders after clicking the "srv" folder, but only one file- so just keep clicking until you see the file "Lafayette", as shown below):



This database file can then be opened to view the various tables/data using the freeware program "DB Browser for SQLite" (<http://sqlitebrowser.org/>)

After opening the lafayette file with this freeware program, and to see all the data in the Reference Monitor table, first select the second tab from left "Browse Data". Then in the "Table" drop-down (just below the tabs) select **log\_ref\_mon\_statuses**

The tables/data shown in the viewer program should also be able to be exported to csv files. But for some reason, I get an error message on my PC when I try to export any of the tables to a file (engineers are able to export them from their PCs).

Please confirm the download icon function works when pressed shortly after performing the clearstats command.

---

### Length of time Reference Monitor data is stored for:

- Refer to the email below from Ron (and in the SecureSync online user guide at the following link, scroll down to "Deleting Temperature Data")

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/OPRTN/TempMon.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm)

- Excerpted below

*"Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten."*

**Email from Ron D (28 Mar 18) (Note- not edited to be directly sent to a customer- except the last paragraph)** The reference monitoring data is stored for the same amount of time as every other graph in SecureSync.

The temperature monitor graph page in the online manual states it. It should probably be added to all of the graph sections that it applies to.

## \*\*Smart Reference Quality Monitoring/Reference 1PPS validation/Yellow PPS Reference status indicator

(Applicable to only versions 5.7.0 and above only)

Refer to online SecureSync User Manual:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/RefMon.htm#Smart](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/RefMon.htm#Smart)

- Smart Phase Monitoring is new feature added in v5.7.0
- Provides 1PPS Phase Validation/Phase Verification of ALL input references (not just the selected reference) using Reference Monitor,
- Provides automatic reference switching to the next lower priority reference/ or coasting of the oscillator for 1200 seconds (while in a force Holdover state).
- Can declare other unselected references as not valid, so that they aren't selected if the currently selected reference becomes not valid.

### Description of Smart Reference Monitoring

Spectracom's Smart Reference Monitoring uses phase error validation in combination with automatic failover:

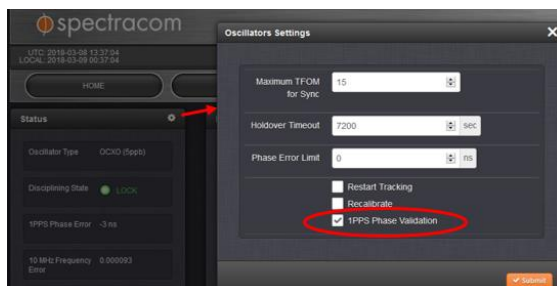
The phase error validation **calculates long-term averages and standard deviations** of the phase offset between the monitored external reference and the internal system reference. The standard deviation is used to calculate two validity thresholds, a higher and a lower one (the latter acts as a hysteresis buffer, preventing the status flip/flopping of the actual phase error validation value varies closely around the outer threshold). The thresholds are not user-configurable.

- A) If the higher threshold value is exceeded, the automatic failover will cause SecureSync to fall back to its next lower reference (if available).
- B) **If no other reference is found, the unit will transition into a 1200-second coasting period.** During this coasting period, the TIME and 1PPS references will continue to be considered valid, but SecureSync's oscillator will flywheel. Note that the PPS reference status light will turn yellow. After expiration of the **1200 seconds**, the unit will transition into Holdover.
- C) Should, however, the above-mentioned higher threshold value no longer be exceeded, the unit will remain in the 1200-second flywheel mode until either (a) the lower threshold value is no longer exceeded, or (b) the **1200-second flywheel period expires**. In both cases, the PPS status light will turn green again.

**Email from Hughes (15 Oct 2018) pertaining to PRN27 signal change:** Spectracom has reported that with the Phase Validation feature turned on, has shown that the 1 PPS jump is minimized to about 100 ns and no 10 MHz jump in holdover during the 10/7 1800 PRN27 event emulation with the GG unit.

### Enable/disable state of Smart Reference Monitoring

- **Disabled** by factory default (upgraded units / units which are cleaned and newly shipped units)
  - “Enabled in the **Management** -> **Disciplining** page.
    1. Press the gear icon to the right of “STATUS” (on the left side of the page).
    2. Select “**1PPS Phase Validation**” checkbox and press Submit



- **Once this function has been enabled:** “Phase measurements and thresholds are dynamically calculated based on the input references statistics”

**Associated Commands** (internal use/reference only)

**NOTE:** “Set” commands are not available to spadmin account (require spfactory). So customers cannot perform any of the calls below used to configure a SecureSync. However, customers can perform the “Get” commands below, using the spadmin account.

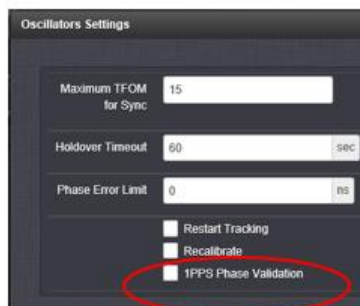
**Note:** these calls were performed on a SecureSync in spfactory account, with included screenshots from the browser- to show the effects of the various calls:

- Verify if Smart Reference Monitor is enabled: **RS\_GetPhaseThreshold 0 all**<enter>

**A) Smart reference NOT ENABLED (Mode = 0 and N = 0)**

```
spfactory@Spectracom /home/spectracom $ RS_GetPhaseThreshold 0 all

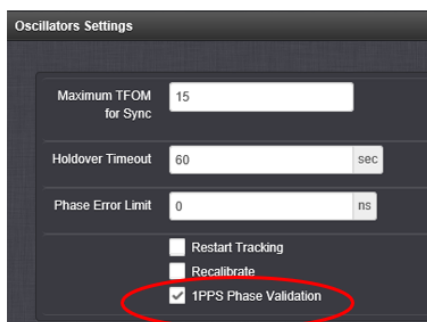
Mode:          0
N:             0
Min Threshold: 999999999.000000
Max Threshold: 999999999.000000
```



**B) Smart reference ENABLED (Mode = 2 and N = 5)**

```
spfactory@Spectracom /home/spectracom $ RS_GetPhaseThreshold 0 all

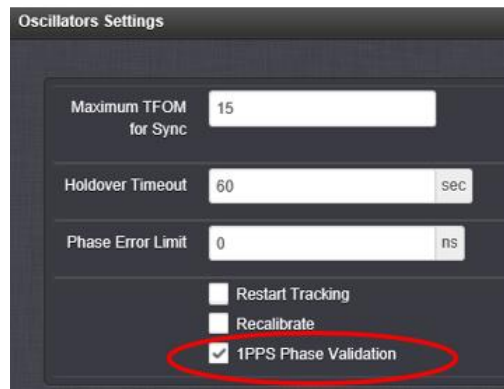
Mode:          2
N:             5
Min Threshold: 999999999.000000
Max Threshold: 999999999.000000
spfactory@Spectracom /home/spectracom $ █
```



- **ENABLE Smart Reference Monitor: RS\_SetPhaseThreshold 0 all 2 5 999999 999999**<enter>

```
Max Threshold: 9999999.000000
spfactory@Spectracom /home/spectracom $ RS_SetPhaseThreshold 0 all 2 5 9999999 9999999

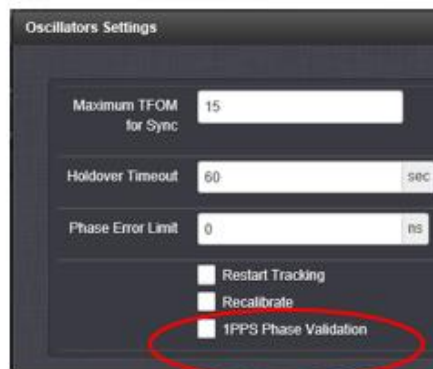
RS (all) Threshold:
Mode:      2
N:        5
Min Threshold: 9999999.000000
Max Threshold: 9999999.000000
spfactory@Spectracom /home/spectracom $ █
```



- **Disable Smart Reference Monitor: RS\_SetPhaseThreshold 0 all 0 0 999999 999999**<enter>

```
spfactory@Spectracom /home/spectracom $ RS_SetPhaseThreshold 0 all 0 0 9999999 9999999

RS (all) Threshold:
Mode:      0
N:        0
Min Threshold: 9999999.000000
Max Threshold: 9999999.000000
spfactory@Spectracom /home/spectracom $ █
```



## Indications of any Reference (selected reference or any others) being declared not valid

### A) Via the “Reference Status table” in the web browser

- Either [Home](#) or [Management](#) -> [Reference Priority](#) pages
- The Reference PPS indicator turns **YELLOW** when declared not valid by smart phase reference monitor.

When the “1PPS Phase Verification” checkbox ([Management](#) -> [Disciplining](#) page) is selected/enabled and a reference is declared “not valid”, its PPS indicator will turn **yellow** (not green or red) as shown below in the example of ASCII input being declared not valid (even though it wasn't the selected reference):

The screenshot shows the Spectracom SecureSync web interface. The 'Reference Status' table is as follows:

| REFERENCE     | PRIORITY | STATUS | PPS    | PHASE    |
|---------------|----------|--------|--------|----------|
| ASCII Input 0 | 1        | TIME   | YELLOW | 3.767 ms |
| GNSS 0        | 2        | TIME   | GREEN  | -15 ns   |
| NTP 1         | 3        | TIME   | RED    | 0 ns     |

The 'ASCII Input 0' row is circled in red, highlighting the yellow PPS indicator and the 'TIME' status.

### B) Via log entries

Example Log entries associated with Smart Reference Monitoring enabled

#### 1. Timing.log

Jan 3 19:06:41 FR2-PQT-M512-309-GM2 FR2-PQT-M512-309-GM2: [system] 2018 003 19:06:41 000 **PHASE INVALID Reference gps0 Restart=0 PPS Valid**

#### 2. osc.log (oscillator log)

Mar 12 12:16:15 HOU-GPS-01 HOU-GPS-01: [system] 2018 071 12:16:15 000 XO: **Phase Reference Valid.**

- A) **Example Osc log entries due to just loss of reception (not due to suspected jamming) for about 8 minutes**

**Note** the logs below were asserted by just disabling GNSS 0 in the Reference Priority table, for about 8 minutes

Feb 11 16:33:17 10 10.2.192.226: [system] 2019 042 16:33:17 000 XO1: Frequency error recalculated: 00.000034 (3.438x10<sup>-12</sup>)  
 Feb 11 16:57:30 10 10.2.192.226: [system] 2019 042 16:57:30 000 XO1: Freq error: phase start: -3.2 ns, phase end: -6.4 ns  
 Feb 11 16:57:30 10 10.2.192.226: [system] 2019 042 16:57:30 000 XO1: Frequency error recalculated: -00.000126 (-1.261x10<sup>-11</sup>)  
 Feb 11 16:58:48 10 10.2.192.226: [system] 2019 042 16:58:48 000 XO: Ref Changed: old=gps0 new=None  
 Feb 11 16:58:49 10 10.2.192.226: [system] 2019 042 16:58:48 000 XO: Phase Reference Invalid  
 Feb 11 17:05:26 10 10.2.192.226: [system] 2019 042 17:05:25 000 XO: Ref Changed: old=None new=gps0  
 Feb 11 17:05:26 10 10.2.192.226: [system] 2019 042 17:05:25 000 XO: Phase Reference Valid  
 Feb 11 17:05:39 10 10.2.192.226: [system] 2019 042 17:05:39 000 XO1: Start Phase Err: +0.1

**associated phase errors during this same time-frame**

|                 |   |   |      |      |       |       |
|-----------------|---|---|------|------|-------|-------|
| 2019-02-11 1... | 1 | 0 | gps0 | gps0 | 37288 | -8    |
| 2019-02-11 1... | 1 | 0 | gps0 | gps0 | 37288 | -7    |
| 2019-02-11 1... | 1 | 0 | gps0 | gps0 | 37288 | -6    |
| 2019-02-11 1... | 1 | 0 | gps0 | gps0 | 37288 | -6    |
| 2019-02-11 1... | 1 | 1 |      |      | 37288 | -211  |
| 2019-02-11 1... | 0 | 0 |      |      | 37288 | -511  |
| 2019-02-11 1... | 0 | 0 |      |      | 37288 | -811  |
| 2019-02-11 1... | 0 | 0 |      |      | 37288 | -1111 |
| 2019-02-11 1... | 0 | 0 |      |      | 37288 | -1411 |
| 2019-02-11 1... | 0 | 0 |      |      | 37288 | -1711 |
| 2019-02-11 1... | 1 | 0 | gps0 | gps0 | 37288 | -1986 |

**B) Example Osc log entries due to due to suspected jamming**

**Note:** the logs below were from a customer's SecureSync with indications of likely jamming resulting in lost reception (for about 800 seconds)

**OSC log**

Feb 6 21:48:31 2019 037 21:48:31 000 XO1: Frequency error recalculated: 00.000013 (1.378x10<sup>-12</sup>)  
 Feb 6 22:14:52 2019 037 22:14:52 000 XO: Ref Changed: old=gps0 new=None  
 Feb 6 22:14:52 2019 037 22:14:52 000 XO: Phase Reference Invalid  
 Feb 6 22:15:01 2019 037 22:15:01 000 XO: Ref Changed: old=None new=gps0  
 Feb 6 22:15:01 2019 037 22:15:01 000 XO: Phase Reference Valid  
 Feb 6 22:15:04 2019 037 22:15:04 000 XO: Ref Changed: old=gps0 new=None  
 Feb 6 22:15:04 2019 037 22:15:04 000 XO: Phase Reference Invalid  
 Feb 6 22:29:43 2019 037 22:29:43 000 XO: Ref Changed: old=None new=gps0  
 Feb 6 22:29:43 2019 037 22:29:43 000 XO: Phase Reference Valid  
 Feb 6 22:29:56 2019 037 22:29:56 000 XO1: Start Phase Err: -25.7  
 Feb 6 22:30:56 2019 037 22:30:56 000 XO1: End Phase Err: -27.6  
 Feb 6 22:30:56 2019 037 22:30:56 000 XO1: Freq Err: +0.000000  
 Feb 6 22:30:56 2019 037 22:30:56 000 XO1: Err Std Dev: +10.1  
 Feb 6 22:32:58 2019 037 22:32:58 000 XO1: Freq error: phase start: -35.9 ns, phase end: -36.4 ns  
 Feb 6 22:32:58 2019 037 22:32:58 000 XO1: Frequency error recalculated: 00.000500 (5.000x10<sup>-11</sup>)

|                     |   |   |      |      |       |    |                 |   |
|---------------------|---|---|------|------|-------|----|-----------------|---|
| 2019-02-01 21:27:30 | 1 | 0 | gps0 | gps0 | 33254 | 13 | 1.3732491424... | 0 |
| 2019-02-01 21:28:30 | 1 | 0 | gps0 | gps0 | 33254 | 11 | 1.3732491424... | 0 |
| 2019-02-01 21:29:30 | 1 | 1 |      |      | 33253 | 9  | 0.0010000000... | 0 |
| 2019-02-01 21:30:30 | 1 | 1 |      |      | 33253 | 15 | 0.0010000000... | 0 |
| 2019-02-01 21:31:30 | 1 | 1 |      |      | 33253 | 21 | 0.0010000000... | 0 |
| 2019-02-01 21:32:30 | 1 | 1 |      |      | 33253 | 27 | 0.0010000000... | 0 |
| 2019-02-01 21:33:30 | 1 | 0 | gps0 | gps0 | 33253 | 29 | 0.0010000000... | 0 |
| 2019-02-01 21:34:30 | 1 | 0 | gps0 | gps0 | 33253 | 29 | 0.0010000000... | 0 |
| 2019-02-01 21:35:30 | 1 | 0 | gps0 | gps0 | 33253 | 2  | 0.0010000000... | 0 |
| 2019-02-01 21:36:31 | 1 | 0 | gps0 | gps0 | 33240 | 5  | 0.0005000000... | 0 |

### Reference Monitor log data/graphs

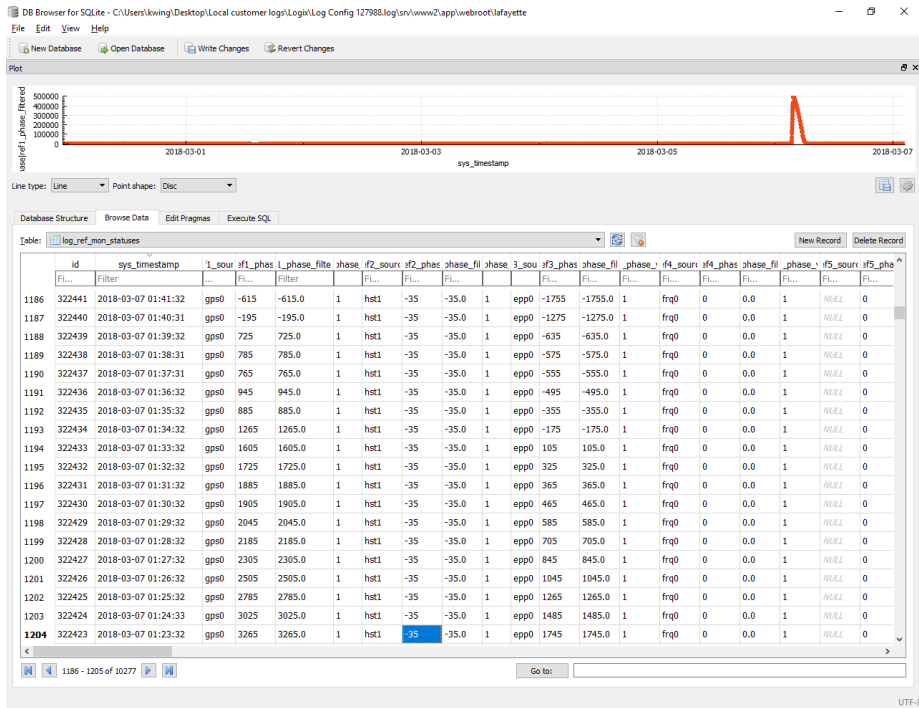
- Phase error values for all input references are stored in the “Lafayette” SQLite database.

The Reference Monitor log data is stored in the SQL database that is in the log bundle (select “log\_ref\_mon\_statuses” in the Table dropdown), or it can be extracted using the “arrow” icon in the upper-right corner of the graph display in the **Management** -> **Disciplining** page of the browser.

|   | id | sys_timestamp   | f1_source | l_phase | ref1_phase_filtered | ref2_source | ref2_phase | ref2_phase_filtered | ref3_source | ref3_phase | hase_f | ref4_source | ref4_phase |
|---|----|-----------------|-----------|---------|---------------------|-------------|------------|---------------------|-------------|------------|--------|-------------|------------|
| 1 | 1  | 2016-09-07 1... | gps0      | -55     | -44.999922547083    | hst1        | 0          | 0.0                 | epp0        | 0          | 0.0    | frq0        | 0          |
| 2 | 2  | 2016-09-07 1... | gps0      | -55     | -48.719615936279    | hst1        | 0          | 0.0                 | epp0        | 0          | 0.0    | frq0        | 0          |

### Three associated fields for each timestamp

- **Refx\_source:** name/number for each input reference
- **Ref phase:** coarse phase error measurement from FPGA (don't use this value)
- **Ref phase\_filter:** accurate phase error measurement (use this value)



**Length of time the Reference Monitor data is stored for:**

- Refer to (in the SecureSync online user guide, then scroll down to “Deleting Temperature Data”) [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/OPRTN/TempMon.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm)

**Email from Ron D (28 Mar 18)** The temperature monitor graph page in the online manual states it. It should probably be added to all the graph sections that it applies to.

“Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten.”

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/OPRTN/TempMon.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm)



## \*\*Input “Reference Status” table

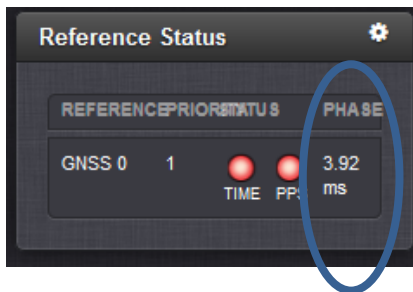
- The SecureSync’s Input “Reference Status” table shows the sync status of all possible input references that SecureSync can sync with.
- Each reference’s phase error is also individually reported in the “Reference Status” table (reported in both [Home](#) and the [Management](#) -> [Reference Priority](#) pages of the browser)

### A) Newer browser (Archive versions 5.1.2 and higher)

#### 1. Versions 5.4.5 and above

Left-side of the [Management](#) -> [Reference Priority](#) page

- Version 5.4.5 enhanced Reference Status with the current 1PPS phase error (to the right of each listed reference)



#### 2. Versions 5.4.1 and below

Left-side of the [Management](#) -> [Reference Priority](#) page



**Potential Issue: Reference Status tables are greyed-out (not red or green)**



- Verify the **Timing System** software version is correct for the **main** software version installed
  - This condition was observed with 5.8.4 installed, and Timing System software at the version for 5.2.1 instead) due to CF card being replaced without a software update being performed.

---

## B) Classic interface web browser (v5.0.2 and below)

Status ->Time and Frequency page

| REFERENCE STATUS |           |           |
|------------------|-----------|-----------|
| Reference        | Time      | 1PPS      |
| GPS 0            | OK        | OK        |
| PTP 0            | Not Valid | Not Valid |
| NTP              | Not Valid | Not Valid |
| User             | Not Valid | Not Valid |
| Local System     | OK        | OK        |

---

### Switching from one input reference to another

SecureSync can be "synced" to more than one reference at a time, with only the highest priority input selected at any given moment. Theoretically, if the highest priority input goes away or becomes not valid, SecureSync will seamlessly transition to the next highest priority without going into Holdover alarm (an entry is created indicating SecureSync switched references). However, Engineering has seen it glitch when switching from one input to another, where the Holdover alarm is generated for one second, and then it's back in sync by the next second. You can let the customer know that the switchover from one reference to another will take no more than one second, as long as more than one valid input is present.

---

### Time to synchronize System Time once an input reference is present and valid

(Questions below were answered by Dave Sohn on 10/11/11)

Q. Does the above time depend on the type (IRIG, ASCII time, NTP) of a reference signal as well?

A. The time for references to become valid from connection of input varies between references, and the state of the input reference. Once a reference is valid and synchronizing the system, the system time will sync within three seconds. The 1PPS may take longer to synchronize depending on the difference between the system and the reference, and is not dependent on which reference is used.

Q. Under the following conditions, how long [s] does the synchronization take?

Difference between SecureSync's time and reference signal's is 1 second:

Difference between SecureSync's time and reference signal's is 1 minute:

A. There is no difference in how long to synchronize the time of the timing system based on the time difference. The time reported by NTP may take additional time depending on the time difference. I don't have estimates for the time to resolve that.

---

## NTP Input

- Refer to the **NTP SecureSync Peering** document for more info :[:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP\\_peering](I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP_peering)

### \*\* “Time Reset” when NTP first starts-up

- Time Steps/Time slews/panic threshold (1000 seconds)
- Refer to **“Time Reset” when NTP starts up** (<..\CustomerServiceAssistance.pdf>) for more details on how NTP initially corrects the time.

### \*\* (HST1) Host disciplining of the oscillator when using NTP as the PPS input reference

- Applicable to TCXO and OCXO only
- Refer to (in this doc: [\(HST1\) Host disciplining of oscillator when NTP or “User set time”](#))

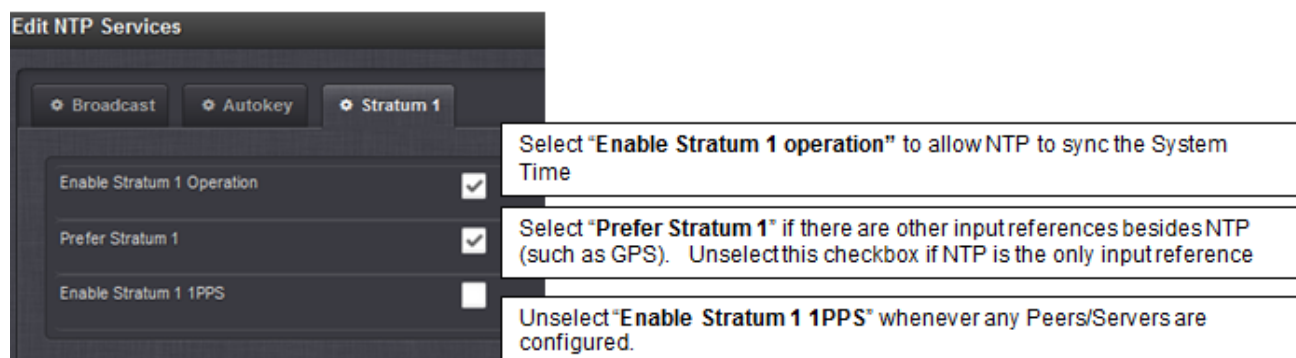
## NTP/External PPS input

- The System 1PPS is controlled by NTP – not by the oscillator (bypasses the oscillator). However, NTP input can be combined with epp0 (external 1PPS input).
- This mode requires a 1PPS input Option Card be installed and changes made to NTP via the Expert Mode). Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP\\_Expert mode-1PPS input](I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP_Expert_mode-1PPS_input)

**Important Notice:** Using NTP and external PPS input as the selected references requires **NTP Expert mode be enabled** so the ntp.conf file can be manually edited. Failure to edit the ntp.conf file in Expert mode degrades the performance of the SecureSyncs outputs (including PTP) and the system does not take advantage of the external PPS accuracies.

## 1PPS synchronization with NTP input - configuration notes

**Management** -> **NTP Setup** page, click on the “Gear” ICON (next to “NTP Services”) and Select the “**Stratum 1**” tab



## Syncing NTP with a SecureSync that is synced via NTP/ External PPS input

- Morgan Stanley is one example of a customer using this mode.
- Make sure SecureSync indicates in sync with NTP/External PPS.
- When syncing NTP via external 1PPS input, NTP Expert mode is required. Must manually change the Atom clock driver (127.127.22.0) value in the ntp.conf file from Stratum 0 to Stratum 1.

Change the “**fudge 127.127.22.0 stratum 0**” line to “**fudge 127.127.22.0 stratum 1**” (no other changes need to be applied).

**Note:** leave Expert Mode enabled or this ntp.conf file will go back to the default values.

- Refer to the User Case examples in the NTP Peering document: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP\\_peering](#)

**Or the Tech note at:**

[EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert mode- 1PPS input\NTP PPS Configuration V4.docx](#)

**Note:** We recommend adding at least two Stratum 1 servers, to avoid a potential condition which might cause NTP to periodically switch between the Stratum 2 server, the System PPS and the System Time (System Time may periodically go into the Holdover mode, making the System Time a valid input to NTP). Listing more than one Stratum 1 server gives the Stratum 1 servers more “weight” so that NTP can always select one of the Stratum 1 servers.

The logs will show **periodic Holdover alarms** occurring, and NTP log will show periodically switching between TSync 0 (System Time), PPS 0 (System PPS) and one or more Stratum 1 servers.

- Note that in at least software versions 5.3.1 and below, Holdover is an Event (entry in the Events log) instead of being an Alarm (entry in the Alarms log)

## **NTP input/1PPS synchronization operation**

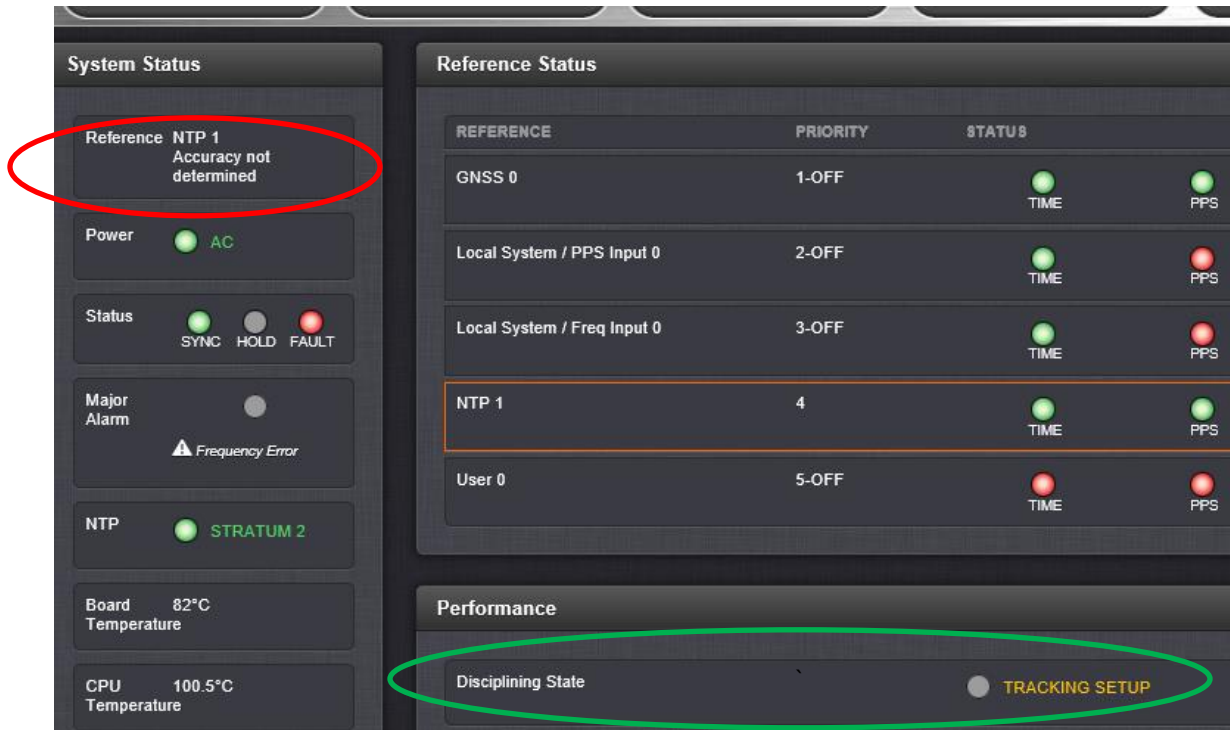
When SecureSync is synced with NTP input, the oscillator’s 10 MHz output frequency is not disciplined (the oscillator is in a free-run mode). Starting once NTP goes into sync and changes from Stratum 16 to a lower stratum (changes to Stratum 2 for example) and then every 60 seconds thereafter, the System 1PPS/1PPS output (1PPS phase error) is stepped about every two seconds into alignment with NTP’s 1PPS to keep it in alignment with NTP.

The oscillator’s 10 MHz output frequency will continue to drift off because the oscillator isn’t being disciplined to an input. TFOM will remain at 15 while synced with NTP input.

With a scope, and after the 1PPS output of the Stratum 2 server finished stepping. I was seeing about 750us to 800us of offset between the Stratum 1 and Stratum 2 server’s 1PPS output. Over time, I was seeing about 20us or so of average periodic jitter on the S2 server’s 1PPS output. On occasion, it went to about 3 to 4ms, but could potentially jump higher.

- The Oscillator Frequency is not disciplined with NTP input (oscillator’s output frequency remains in free-run mode).
- TFOM will start at the value it was at, just prior to NTP sync. Then it will increase as the oscillator continues to drift while synced to NTP.
- So if it was synced to GPS at Stratum 3 when switching to NTP sync, TFOM will start at 3 and then slowly ramp up.

“Accuracy Not determined” (reported top-left corner of *Home* page, under “Reference” field)

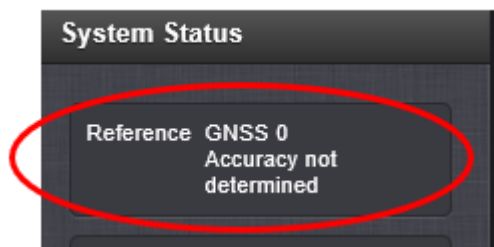


**NOTE:** “Accuracy Not determined” is **NOT** reported after each reboot, until an external reference has been selected (instead, it reports “Reference None” at boot-up, until a reference is selected)

1. IF the unit hasn’t previously synced to another external input reference (since boot-up) before syncing to NTP input, TFOM will be (and will remain) “**TFOM 15**”, unless it switches to another external reference (such as GNSS 0) sometime thereafter (“**Accuracy Not determined**” will be indicated, until it switches to an external PPS such as GNSS 0).

The Oscillator “**Disciplining State**” remains in “**Tracking Setup**” mode (as shown above in green circle)

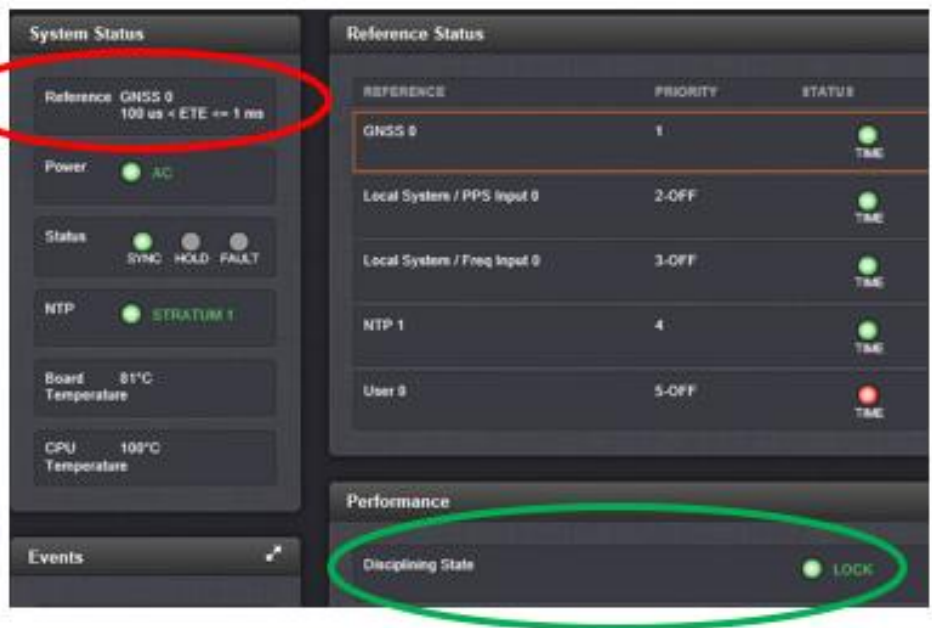
“**Accuracy not determined**” will remain reported for a short time, while showing a selected reference (such as GNSS 0, for instance)



“**Accuracy not determined**” may remain momentarily reported, after first selecting an external reference (such as GNSS 0, for instance), while the oscillator is “**Tracking Setup**” mode (in the process of locking to the PPS input)

Once the oscillator has switched to “**LOCK**” to an external PPS reference (such as GNSS 0) for the first time, it

will then switch to reporting an “ETE value” (no longer reporting “Accuracy not determined”)



TFOM is reported in the browser/CLI:

A) Newer browser: [Management](#) -> [Disciplining](#) page

B) Classic interface: [Status](#) -> [Time and Frequency](#) page

C) CLI interface

- CLI command for TFOM: `SS_GetTfom 0 <enter>`
- CLI command for reading the MaxTFOM value `SS_GetMaxTfom 0 <enter>`

- “1PPS Phase Error” will continue to report “1 Sec” (linked to TFOM not being measured) if SecureSync hasn’t previously synced to another external reference, such as GPS. Then it will increment from there.
- With NTP input being a lower priority input reference, a 1PPS jump will occur about a minute after losing a higher priority reference (holdover for about a minute and then NTP kicks in, causing the 1PPS to jump).
- As typical, NTP output accuracy is like 1-10ms, 1PPS output/System Time/on-time point will have more jitter than with GPS input.
- Due to NTP Stratum 2 offset between the S2 server and its selected S1 server, the 1PPS/on-time point will be delayed from the on-time point of its reference by about a 1ms processing delay PLUS the NTP offset value (if NTP offset is 50ms because of lots of hops, the offset between the on-time points will be about 51ms).
- NTP input does not become a “valid” reference, until the Linux kernel has been corrected (second round of NTP sync has to have occurred- so it doesn’t go valid until the second time it goes into sync). KTS timing engine does not use it for a reference until this second sync.
- User and NTP references only go “valid” when they become the “selected reference”. They do not remain valid if they aren’t selected (they remain not valid when they aren’t selected. with NTP, it’s the selected reference, when NTP selects another Time Server to be its selected reference (as displayed on the [NTP-> Status](#) page or in the NTP log).

The reason it does not remain valid is because NTP can be an input or an output, but not both at the same time. So,  
pg. 782

NTP switches to output mode and is then toggled back to input mode again (so it's not a constant input reference).

**Note:** NTP may periodically and temporarily select an NTP server (before switching back to the System Time reference, for example). In this scenario, NTP will go momentarily valid and then back to not valid again, because NTP is no longer synced to another NTP server.

Even though it's normally displayed as "not valid", NTP inputs from other NTP servers are checked for validity each second, allowing NTP to become the selected reference within one second of losing all higher priority references (it doesn't have to wait to be re-qualified, when all other higher priority references are lost. Instead, it can switch over to NTP "right away").

### Questions from *TOYO* - answers from Keith (8 Jan 15 based on 5.1.7 software)

Q And customer measure phase change of 1PPS from SecureSync by comparing phase difference between 1PPS of SecureSync and 1PPS of sample itself. But as soon as SecureSync sync to stratum1 NTP server(ntp.nict.jp), this phase difference start to expand.

[Question]

1. Could you please let us know possible cause of this symptom?

**Keith's response:** In summary of the below information, the observed phase change of the 1PPS output is a direct result of the 1PPS output being aligned with the NTP reference.

When SecureSync is synced via NTP input, the oscillator's 10 MHz output is not disciplined. The oscillator remains in a free-run state, and the TFOM value starts at the value it was at, when synchronization occurs (with no other input references syncing it first, the TFOM will remain at 15). In this configuration, once NTP has fully synced and is no longer at Stratum 16 (and continuing every 60 seconds thereafter) its 1PPS output (System PPS) is step-adjusted to the internal 1PPS being generated by the NTP input. This is to maintain alignment of the System PPS to the NTP reference.

The phase change of the 1PPS output from the SecureSync when compared to the sample after NTP went into sync is the system adjusting the SecureSync's 1PPS to be in alignment with the NTP 1PPS (in small steps about once every two seconds). This alignment/ adjustment can't start to occur until after NTP within the SecureSync has gone into sync and its NTP is no longer Stratum 16 (When it's syncing to a Stratum 1 server, this alignment process starts when SecureSync's NTP goes to Stratum 2 for instance).

2. Could you please let us know how 1PPS output from SecureSync is affected by syncing to stratum1 NTP server?

**Keith's response:** Once NTP goes to stratum 2 in the SecureSync, the SecureSync's 1PPS output will be stepped as necessary to bring it into alignment with the NTP's 1PPS reference. This continues to occur every 60 seconds as long as the SecureSync continues to remain synced via NTP input in order to maintain the alignment of the System PPS with the NTP reference.

Note that as the NTP reference's 1PPS inherently has much more jitter than the 1PPS from GPS input, this will translate into more System 1PPS jitter than when the SecureSync is synced via GPS instead of via NTP.

3. Could you please let us know how 10MHz output from SecureSync is affected by syncing to stratum1 NTP server? (I do not know what Sampler is using 10MHz output from SecureSync for. But please let us know behavior of 10MHz from SecureSync when syncing to stratum1 NTP server.)

**Keith's response:** The oscillator's 10 MHz output is not disciplined while the SecureSync synced to NTP. The oscillator remains in a free-run mode with its 10 MHz output frequency drifting off at the typical drift rate of the oscillator. The better the type of oscillator installed, the less frequency drift that will occur. Because the oscillator is not being disciplined with NTP input, its frequency is not being corrected back to an accurate 10 MHz to account for drift, as it normally does when the input reference is GPS, for instance.

---

## DSCP values for NTP

Q I was analyzing network traffic and noticed that our clock is sending NTP responses to client requests at a QoS DSCP value of 46. This puts in our priority voice queue. I've looked through the GUI for a way to modify this setting but haven't been successful. Can you tell me how I can change this QoS value in the GUI or CLI? Thanks. As an alternative, we will configure the Cisco switch port inbound policy for the change in DSCP.

**A reply from Dave L (26 Sept 16)** DSCP values for NTP can be adjusted in NTP expert mode. By default, NTP 4.2.8 uses a DSCP value of 0x2e (46) for expedited forwarding. The DSCP value can be adjusted by adding the below line in the config file in expert mode.

```
dscp <value>
```

For instance, to change the DSCP value to 0x30 (48) CS6 add the below line

```
dscp 48
```

**(addition from Keith 25 March 2019)** For more information on enabling NTP Expert mode, please refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_ExpertMode.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_ExpertMode.htm)

Note the NTP Expert mode needs to remain enabled in order for any changes incorporated in the ntp.conf file to persist. Disabling Expert mode reverts any changes which have been made to this file

### Log entry for reporting the selected NTP server it's synced with

Q. Is there any logs that show where it has synced its time from the other NetClock. I have looked through all the different logs, but can't find it if there is one.

**A Reply from Keith (6 JAN 15)** Regarding the unit's logs indicating that it's synced with the Model 9383, the only available entry for indication that it's in sync with another NTP server is in the "Events" log which will report "**Reference Changed to Time Ref: ntp PPS Ref: ntp**" (as shown below). But it doesn't log the specific IP address of the time server it's synced with.

| Id  | Date            | Entity   | Message                                                                   |
|-----|-----------------|----------|---------------------------------------------------------------------------|
| 174 | Jan 07 20:11:07 | [system] | No Longer In Holdover                                                     |
| 173 | Jan 07 20:11:03 | [system] | Reference Change (Cleared)                                                |
| 172 | Jan 07 20:11:02 | [system] | Reference Change                                                          |
| 171 | Jan 07 20:11:02 | [system] | 2015 007 20:11:01 000 SS: Reference changed to Time Ref: ntp PPS Ref: ntp |
| 170 | Jan 07 20:11:00 | [system] | Reference Change (Cleared)                                                |
| 169 | Jan 07 20:10:59 | [system] | Reference Change                                                          |



### \*\*\*Issues with NTP Stratum synchronization

#### A) Holdover mode occurring while still receiving NTP timestamps from another time server

- Refer to report (“MS\_NTP\_Testing\_July 2019.pdf”): <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\NTP\NTP stress testing\our NTP Stress test results>
- if NTP is the only input reference, and if SecureSync is being pounded with over ~7000 NTP requests/second, SecureSync can be inadvertently placed into Holdover mode, due to the E100E driver added in versions beyond 5.8.2 (or patch installed with version 5.8.2),

#### B) Excerpt below from load test report alluded to above

##### Root Cause:

This issue is occurring because NTPD is not responding to NTPQ queries which are performed to determine if the SecureSync is still in sync to its’ NTP server. Because the device can not determine if it is in sync, it goes into holdover.

It was determined that the cause of this issue was because of a change in one of the following pieces of software: the kernel, NTP, or the 1204-06 e1000e driver. To test which component was the root cause NTP stress was applied to a SecureSync as the versions of these items were changed, and it was recorded whether it went into holdover.

#### C) Table 2. NTP Stress Testing (while varying software versions)

| SecureSync NWP Version Equivalent | Kernel Version | NTP Version | E1000E Driver Version | SecureSync NWP Version Equivalent | 20k packet stress test result: |
|-----------------------------------|----------------|-------------|-----------------------|-----------------------------------|--------------------------------|
| 5.7.1                             | 4.4.26         | 4.2.8-r10   | 3.2.6-k               | 5.7.1                             | No Holdover                    |
| 5.8.2                             | 4.14.34        | 4.2.8-r10   | 3.2.6-k               | 5.8.2                             | No Holdover                    |
| 5.8.2 (with e1000e patch)         | 4.14.34        | 4.2.8-r10   | 3.4.2.1-SPEC          | 5.8.2 (with e1000e patch)         | Holdover                       |
| 5.8.5                             | 4.14.34        | 4.2.8-r12   | 3.4.2.1-SPEC          | 5.8.5                             | Holdover                       |

In conclusion, the patched e1000e driver is the reason the SecureSync is going into holdover. Prior to the e1000e driver being patched, NTP was not responding to all queries due to the driver restarting. This resulted in more processing power being available as it was not meeting load requirements. With the driver patched, NTP is responding to all the queries within its capacity, and under load (above 7,000 request per second) we see that the status queries are starved out, resulting in the appliance going into holdover.

#### D) Periodic large 1PPS jumps (like ~300ms) in 1PPS phase error/NTP periodically goes to Stratum 16

- Make sure the “Prefer Stratum 1” checkbox is NOT selected if NTP is the only input reference available (no GPS input for instance).

**Email from Keith (9 Jan 15)** Besides periodically losing NTP time stamps (which doesn’t sound like is occurring in this case), the only other thing I can think of is to unselect the “Prefer Stratum 1” checkbox.

Navigate to the **Management -> NTP Setup** page of the browser, click on the “Gear” ICON (next to “NTP Services”) and Select the “Stratum 1” tab. Unselect the “Prefer Stratum 1” checkbox (leaving just the “nppt Operation” checkbox selected in this tab).

This checkbox puts more weight on external references such as GPS for NTP’s sync. With NTP being the only input reference, NTP may periodically switch to another free-running clock as its reference (temporarily making NTP go to Stratum 16) and then switching back to the 9383 again (allowing NTP to go back to Stratum 2 again). Note that after pressing Submit, NTP will automatically restart and resyncs just a couple minutes later (there is no need to manually stop/restart NTP for this checkbox change to become effective).

---

**E) Nearly one second (0.99xxx) potential System Time (1PPS output jumps when syncing via NTP input**

- Refer to Salesforce case 14648 (<https://na8.salesforce.com/500C000000ZhjGW>) for Open Access
- Potential “edge” issue starting with new version of NTP (v4.2.6) in versions 5.0.0 through 5.1.4 (should be fixed in version 5.1.5 and above updates)
- Can result in periodic one second time jumps and time corrections back sometime later
- Temporary fix is patch update version 5.1E
- Fix expected to be included in the next software update (anticipated as version v5.1.5) (UPDATE: 9 Jan 5
- KW – I confirmed with Dave Sohn this fix was added to the software as of at least 5.1.7 if not earlier).

---

## PTP Input

- Refer to SecureSync Option Card information document for more information <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf>

---

## IRIG input

- Refer to SecureSync Option Card information document for more information <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>
- Requires IRIG Input/Output Option card be installed in the SecureSync

---

## \*\*Time Synchronization for Secure Networks using fiber

- Refer to: <http://www.spectracomcorp.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=1606&PortalId=0>

---

## Using a DAGR as an input reference to Sync SecureSync

- For more information on using a DAGR with Model 1200 or 2400 series SecureSyncs, refer to the “DAGFR” section of the SecureSync Option Card information document for more information <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf>

---

## HaveQuick/Stanag input

- Requires Havequick/Stanag Input/Output Option card be installed in the SecureSync
- For more information on Stanag/Havequick, refer to the SecureSync Option Card information document for more information <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf>

---

## ASCII Input

- Requires ASCII RS-232 (1204-02) or RS-485 (1204-04) Input/Output Option card be installed in the SecureSync
- For more information, refer to the 1204-02 or 1204-04 sections of Option Card information document <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf>

---

## Manually setting the System Time (User/User “self” mode)

- The “User” reference can be combined with another reference, if desired (such as user/External PPS for instance). But manual intervention is still required to make it a valid reference. For no manual intervention

need to use the “Local System” reference instead of “User” reference.

**NOTE: USER/USER** mode MUST be enabled in the reference priority table in order to be able to manually change the date/time via the web browser, CLI interface (such as dateset or doysel) or front panel. If USER/USER is not enabled, the time/date will not be changed.

**(Host mode):** “One time use only” input reference to allow a user to set the time. If unit power cycles or if it selects a higher priority input and then loses all higher priority inputs, the time has be manually set by the user in order for this reference to be valid again.

**“Per Dave Sohn (14 JAN 15) “USER” can be combined with other input references (such as GNSS 0 /USER or USER /GNSS 0 as two examples). This is similar to “Local System” reference, but USER requires manual input for validity.**

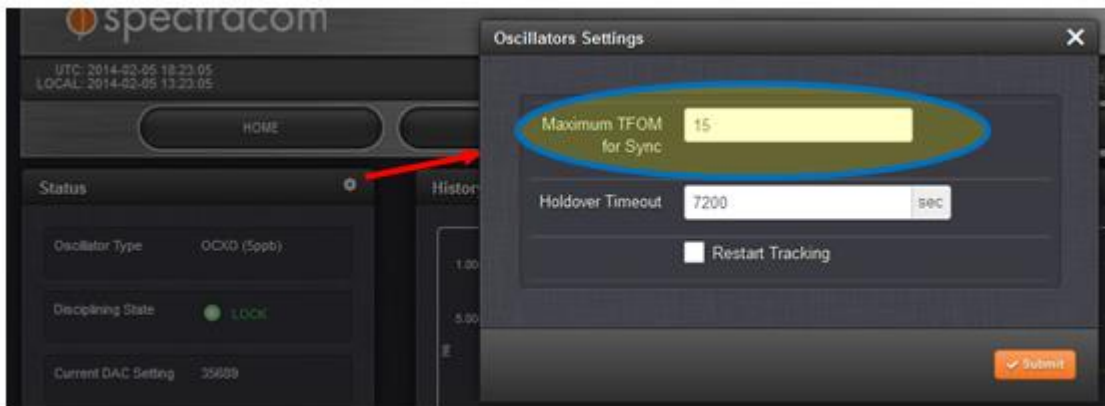
**Note:** (applicable to TCXO/OCXO with versions 5.3.0 and below installed, and RB oscillators) While in Host mode (time manually set and no higher 1PPS inputs with a higher priority), there is no external reference to use for monitoring the oscillator frequency. Therefore, the Freq Error (Frequency Error alarm) will remain asserted and the Fault LED will remain solid red. It can only be cleared by applying an external 1PPS reference (it remains asserted until an external 1PPS input reference becomes available).

- TFOM with User set time will be 15. If MaxTFOM is set to less than 15, User/User mode will not allow SecureSync to go into Sync.

**Important note:** any customer intentionally manually setting the System Time ahead or back should have an Archive version of 4.8.4 or higher installed. A large manual time change to the System Time will cause NTP to stop syncing altogether, if NTP has no other available references to sync to. Version 4.8.4 added a mechanism that monitors NTP state and restarts it if it detects it’s in this state.

### A) Versions 5.1.2 and above

- Configured in the Management -> Disciplining page and then clicking on the “gear” next to “Status”
- Make sure Max TFOM is set to 15



### B) Versions 5.0.2 and below Setup -> Disciplining page)

- Enable User/User mode in Setup -> Reference Priority page (Entry is present but disabled by default)

**Note:** If Max TFOM is lower than 15, User/User will be “OK” but Sync Status will not go to “OK”

1. Hit Submit on **Management -> Time Management** page.
2. Synchronization should go to “OK”
3. TFOM value will remain at 15 (reported on Status -> Time and Frequency page).
4. The Oscillator is not disciplined with NTP input (oscillator remains in free-run mode).

## Linux Kernel time

- Refer to Mantis case 0001704 for more info.
- The battery-backed Real Time Clock (RTC) is read upon each boot-up in order to set the Linux kernel time.
- The kernel time then sets the KTS time.
- The kernel time is adjusted by NTP during synchronization to other references.
- Fcron (scheduler program) runs every 10 minutes to write the linux time to the RTC.
- Upon a Reboot or halt being performed, the kernel time is set into the RTC.

**Note for versions 4.8.9 and below** (see “Update” below about versions 5.0.0 and above) If the time is manually set, KTS is set to this new time. NTP will start to adjust the kernel time. If the time is manually set backwards by any amount, Fcron may stop running until time catches up, and therefore it may not set the RTC. If the unit is then power cycled (not Rebooted or Halted), the manual set time is lost upon reboot. In order for the manual set time to be retained for the next power-up, a Reboot or Halt needs to be performed.

- **Update:** this issue above was reportedly fixed in the version 5.0.0 software update. Refer to Mantis case 2091 (<http://cvsmantis.int.oroia.com/mantis/view.php?id=2091>)

## Holdover Mode while in User mode

- DAC value (reported in discstats) should remain constant when in user set time

After sync has occurred when using the User mode, the time server does not go into Holdover mode thereafter. It remains in full sync mode. So the Holdover timeout value doesn't apply to this mode. The Holdover timeout only applies if a higher priority reference becomes valid sometime after the User reference has gone valid, and then the higher priority reference(s) is lost. The unit will then go into Holdover mode.

## Software Issue with LPN oscillator potentially intermittently being disciplined (DAC value changing) with no external input applied (oscillator is actually supposed to remain in free-run mode)

- Refer to Mantis case 3090/Salesforce case 18770
- Observed in v5.2.1. Should be fixed with 5.3.0.
- Caused devices syncing to it to observe a large 1PPS phase error a while after initial sync.

## System PPS while in User mode

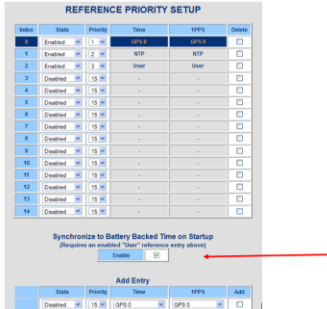
- System PPS starts at the arbitrary spot it's at when the time is hand-set by a user (it can be off by +/- 500ms)
- With the oscillator being in free-run, System PPS will then start to drift.
- If an higher priority external reference then becomes present/valid, the System PPS will jump to the reference (not slew like it normally does when switching references that aren't aligned with each other)
  - Because the other device(s) already synced when the time was first hand-set, devices syncing to the SecureSync will see a large shift in their input reference from the SecureSync. This may adversely affect their operation, resulting in logs/alarms being asserted (with Spectracom devices, such as the Frequency Error alarm for instance).

**Email Keith sent to Sylvain (5 Feb 2013):** You can certainly manually sync the SecureSync to itself, allowing the NTP stratum to go to Stratum 1. This is known as the “Self” input reference. Once the Self/Self reference has been enabled in the **Setup->Reference Priority** page of the browser (it is disabled by factory default), a user is then allowed to manually set the System Time and Date, as desired (as configured in the **Setup -> Time Management** page of the browser).

Once the time has been manually set, SecureSync will go into Sync and NTP will go to Stratum 1 within just a couple of minutes

thereafter. As long as the SecureSync isn't power cycled, and as long as no higher priority references become present/valid, SecureSync will remain synced to itself, allowing NTP to continue to report it's at Stratum1.

To alleviate the need for a user to manually set the time after each boot-up, the "Battery Backed Time on Start-up" feature can be enabled (in the **Setup -> Reference Priority** page of the browser. With this checkbox selected, SecureSync will automatically go back to Stratum 1 shortly after each boot-up (no user interaction is required). The time/date that is used for synchronization is the time from the Real Time Clock, which "maintains" an approximation of the correct time/date while the system is powered-down.

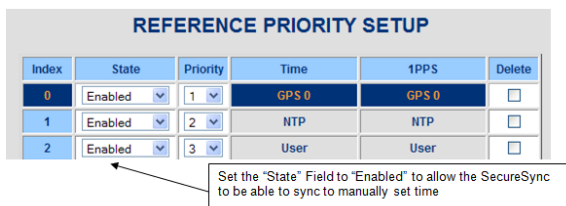


The ability to manually set the time/date of the SecureSync ("Self" mode) and the "Battery Backed Time at Start-up" feature is discussed in the "Reference Priority Use Case Examples" in the SecureSync manual. Refer to "Example 4", starting on page 3-53 of this manual.

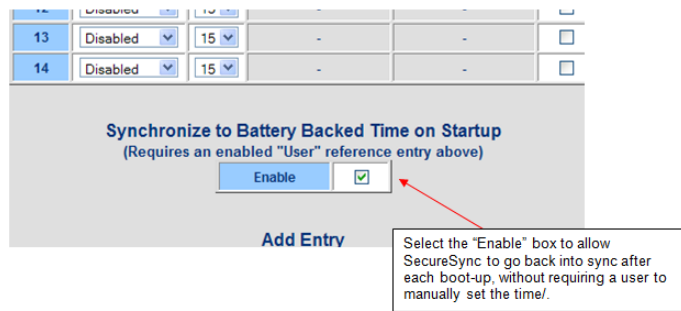
**Email from Keith to a customer (26 Apr 2013)** If it's desired to manually set the time of the SecureSync, instead of syncing it to an external time reference such as GPS, this can be performed via the Setup -> Time Management page of the web browser. It can also be performed using a telnet/ssh session or by using the front panel keypad/LCD window ("Clock" menu).

#### Notes about manually setting the time:

- 1) The "State" field User/User entry (row) of the Reference Priority table needs to be enabled (by default, its set to disabled). This table is configured in the **Setup -> Reference Priority** page of the browser (this table can also be configured using SNMP Sets).



- 2) If there are any higher priority input references that are present and valid, they will override and correct the user set time/date. Any other reference that may be present can be disabled in the Reference Priority table, if desired to keep it from overriding the manually set time/date. This configuration change alleviates the need to have to physically disconnect an input from the NTP server.
- 3) Unless the "**Synchronize to Battery Backed Time**" checkbox underneath the Reference Priority page of the browser is selected, the time needs to be manually set after each boot-up, in order for the SecureSync to go back into sync. When this box is selected, the SecureSync will go back into sync automatically after each power-up, without requiring a user to have to manually set the time to achieve sync status again.



## Manually setting the System time backwards into the past

- When System Time is advanced into the future, RTC is updated every 10 minutes.
- When System Time is set back into the past, RTC isn't updated the first time for about 3 to 4 hours. Then its updated every 10 minutes again.

The system is not intended to be a simulator. It especially does not like being set backwards to an earlier time. This causes Cron to completely stop running, until time has caught up to the correct time.

If the time is set backwards and then power cycled without a several minute delay, it will not power-up with the time that it was manually set to. It takes several minutes for NTP to change the kernel time, once it's been manually set. Then cron, which is used to periodically set the RTC stops running until time catches up to the kernel time. If the time is set backwards, a delay of several minutes (like 20 to 30 minutes) should occur between setting the time and power cycling the unit.

**Email Keith sent to Masataka (18 Feb 15)** Thanks for your email. Our Applications Engineering team has reviewed the information you provided us with regards to the SecureSync's RTC being saved. I am happy to pass along to you their findings.

To begin, when manually setting the time of the SecureSync, there is a one particular scenario that will allow the RTC to be automatically saved within 10 minutes of setting the time. There is another scenario which prevents the System Time from being able to be automatically saved to the RTC for a few hours, unless a reboot or halt of the SecureSync is commanded.

If the System Time/date is manually set by a user to a time/date ahead of the current System Time, the SecureSync continues to be able to automatically set the time into the RTC every 10 minutes (on a 10 minute schedule). However, if a user manually sets the date/time to an earlier date/time than the System Time was set to, the System Time can't be automatically set into the RTC for about 3 to 4 hours, unless a *reboot* or *halt* command is performed.

If the date/time is set by a user to a date/time in the past and its desired to save this "new" date/time into the RTC without waiting the 3 to 4 hours for it to be automatically saved, the SecureSync should be commanded to be either rebooted or halted (not just power cycled) after setting the date/time backwards. Note the RTC is not updated upon a power cycle of the SecureSync. However, the RTC is updated with the System Time upon either a reboot or a halt command being issued. The SecureSync can be either rebooted or halted via the front panel menus, the web browser, the CLI command line interface or via SNMP.

Please be aware that the RTC taking a few hours to be set when a user sets the date/time into the past is not a software bug and Spectracom has no intentions at this time of changing how this operates. If it's desired to manually set the time of the SecureSync backwards to a previous date/time for some reason, the SecureSync should be either rebooted or halted (via its user interfaces) in order to alleviate the need to wait the 3 to 4 hours that is needed for the RTC to be updated with this earlier System Time. Note that the RTC is updated with each reboot or halt command, whether the date/time was set forward or backwards from the starting System Time. The reboot/halt command alleviates any need to wait for the RTC to be updated, as the RTC update occurs before the SecureSync is brought down with either command being performed.

---

## Enable Battery Backed Time (time sync immediately upon boot-up)

### Configuration

- The button selection is stored in the “**rmsf.conf**” file (/config directory)

|           |                                   |                                                                                       |
|-----------|-----------------------------------|---------------------------------------------------------------------------------------|
| rmsf.conf | Enable battery-backed time button | <b>Startupsync 0:</b> button not selected<br><b>Startupsync 1:</b> button is selected |
|-----------|-----------------------------------|---------------------------------------------------------------------------------------|

---

### Log entries asserted for enabling/disabling Battery Backed time checkbox in browser

#### Journal log

- In 5.8.9, confirmed no log entries asserted in Journal log, for enabling or disabling.

#### Timing log

- Whether or not battery backed time is enabled: **HR: Enabling Host Set Time Mode.**

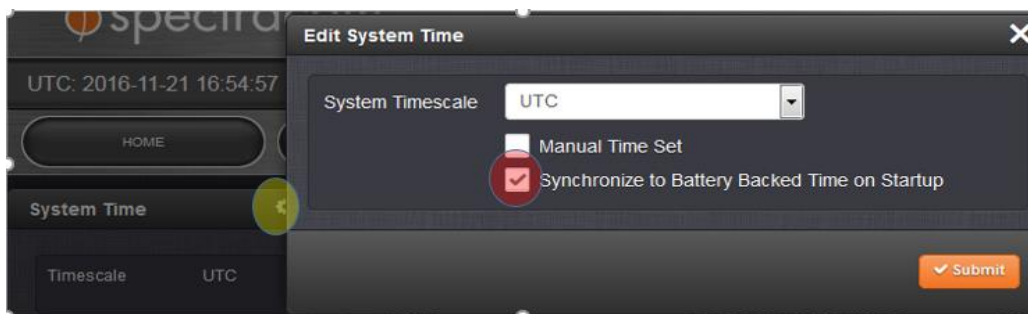
---

### Web browser

#### A) New browser

- **Management** -> **Time Management** page of the browser.
- Click on the gear-box next to “**System Time**” (top left corner)

The “**Synchronize to Battery Backed time on Start-up**” checkbox can be selected as desired (as shown below) in the **Management** -> **Time Management** page of the browser (first press the “**gear**” icon to the right of “**System Time**” in the upper-left corner of the page to open the pop-up window)

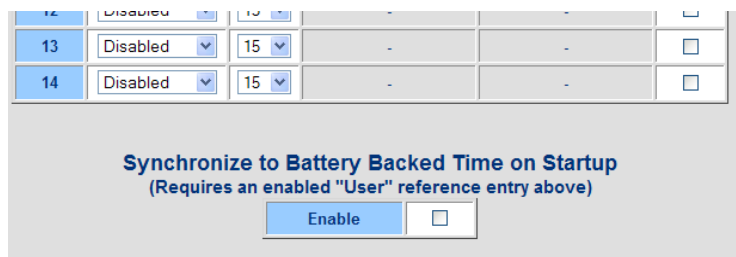


#### B) Classic Interface browser

Starting in version 4.8.0, customers will have the ability to have SecureSync sync to itself upon each reboot. For those customers that don't care about accurate time, this new feature prevents the user from needing to manually set the time, each time SecureSync reboots. It will now happen automatically, if they select the box under the Reference Priority table.

Checkbox to enable this feature (default is not selected) is located on the Setup /Reference Priority page of the browser:





A log entry is created in the System log that the unit synced to itself and is not traceable.

Important Notes:

- 1) The Input reference priority table needs to have an enabled row that has "User" defined as a "Time" reference, in order to use this capability.
- 2) If a higher priority reference becomes available anytime after initial time sync has occurred (such as GPS, for instance), the input reference will may cause a time jump to occur while SecureSync is already in sync (if the RTC is not correct when it boots-up). The amount of time change will be dependent on how long the unit was powered down for and if it was in sync, before it was last powered down.

Q. What would the daily drift rate be with an undisciplined OCXO?

**A. (from Dave Sohn on 11/29/11):** The daily frequency aging of the standard OCXO is 5.00E-10. The daily frequency aging of the high-performance OCXO is 2.00E-10.

The daily drift will be a combination of the initial frequency error, which is unknown for an undisciplined system, and the increasing effects of the frequency aging. The actual offset will also include the initial phase offset of the 1PPS, which is also unknown for an undisciplined system.

## Local System reference (Self Reference)

- Local System is the "Self" reference as referred to in the Tsync boards
- Local System can be used as EITHER the Time OR the PPS reference, but NEVER as both references.
  - **Local System/Local System:** Not a valid combination. Local System has to be combined with a different time reference or 1PPS reference in order to be a valid (internal) reference.

Tsync-PCIe can be "synced" to more than one reference at a time, with only the highest priority input selected at any given moment. Theoretically, if the highest priority input goes away or becomes not valid, SecureSync will seamlessly transition to the next highest priority without going into Holdover alarm (an entry is created indicating SecureSync switched references). However, Engineering has seen it glitch when switching from one input to another, where the Holdover alarm is generated for one second, and then it's back in sync by the next second. You can let the customer know that the switchover from one reference to another will take no more than one second, as long as more than one valid input is present.

## NTP operation while in User/User mode

**Note:** Per Ron Dries, NTPMOND "wakes-up" every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resyncs and be useable again.

- Manually changing the System Time by 1 second or greater will cause NTPMOND to automatically stop and restart NTP to account for the time change of the NTP input
- NTPMOND stopping and restarting NTP is logged in the system.log (not the ntp.log)

[system] ntp monitor stopping ntpd, found 3590 second difference (NTPMOND)

followed by:

[system] ntp monitor restarting ntpd (NTPMOND)

**NTP.log** entries also asserted:

ntpd [xxxx] ntpd exiting on signal 15

followed by

ntpd [xxxx] "127.127.1.0 interface 127.0.0.1 -> (none)

---

### Issue with NTPMOND trying to stop NTP when error >1 second

Version 5.3.0 update (~Sept 2015) fixed issue caused by NTP monitor Daemon NTPMOND, trying to stop NTP when the Timing System and Linux kernel time differ by more than 1 sec

### **NTP step threshold (NTP's Reference time change limits)/ ntpmond restarting NTPD**

- Refer to <http://doc.ntp.org/4.1.2/debug.htm>
- Default step threshold is **128 milliseconds or less**
- Default stepout threshold (how long the error has to exceed the step threshold before NTP steps - after NTP is already running) is 900 seconds.
- The step threshold can be changed by the tinker step command (refer to "tinker" at <http://doc.ntp.org/4.1.2/miscopt.htm>)

### **NTP Step threshold (128 milliseconds)**

#### **A) Initial NTP startup**

- If the initial time error is greater than 128ms - NTP is allowed to step (correct) the time right away.

#### **B) After NTP is already running**

- If a time error is greater than 128ms, normally NTP would have to wait 900 seconds (15 minutes) with this large of an error before NTP steps (due to the default stepout threshold).
- But our NTPmond daemon checks NTP every 16 seconds and restarts NTP if the error is greater than 1 second. So NTP can step the error much sooner than usual (it doesn't have to wait 900 seconds before correcting the time).

### **NTPmond restarting NTP if time offset greater than 1 second**

- NTPMOND "wakes-up" and check NTP every 16 seconds to check if NTP is running and if it's within 1 second of the System Time (while synced to System Time).
- NTPMOND will restart NTP if NTP is in sync and the time error from KTS is 1 second or greater, or if NTP exceeded sanity limit of 1000 seconds (16min 40 sec) which can cause it to stop running

**Note:** Per Ron Dries, NTPMOND "wakes-up" every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resyncs and be useable again.

### **NTP also has its own Reference time change limits, as well (NTP step threshold of 128ms)**

- If NTP's selected input changes by **128 milliseconds or less** NTP **slews** to the reference. (maximum rate of 500 microseconds per second-which is about 4 minutes to slew 128ms)

#### **Fastest time to slew**

**500us** = 1 second

**1ms** = 2 seconds

**64ms** = 128 seconds (2.1 minutes)

**28ms** = 256 seconds (4.2 minutes)

- If NTP's selected input changes by **more than 128 millisecond**, NTP **steps** to the reference.

**Use the `ntpq -p` CLI command to report the current time offset between NTP and the System Time (KTS)**

- Perform an `ntpq -p` (or `ntpq -pn`) in CLI and look at the Offset value of "PCI\_TSYNC(0)" (or "10.2.100.45.0")
- The initial time offset will vary after every reboot/power cycle (can be up to 1 second off).
- The offset can be less than or greater than 128ms after each boot-up.
- If the "offset" of "tsync\_pci(0)" is less than 128ms, it can take NTP a few minutes to slew to the correct time (fastest possible slew rate is 500 microseconds per second- about 4 minutes to slew 128ms).

---

## STL \*(Satelles) “Resilient PNT” input Option Card (Option Cards 1204-3E and 1204-3D)

- For all details, refer to SecureSync Option Card Model 1204-3E/1204-3D in the SecureSync Option Card info document: [..\SecureSync Option Card information.pdf](#)
- For general info on STL, refer also to STL tech note: [I:\Customer Service\1- Cust Assist documents\Satelles resilient PNT.pdf](#)
- STL info on our website: <https://spectracom.com/resources/essential-education/what-is-stl>

### GPS antenna alarm asserted

- This alarm is only associated with the GPS receiver
- If GPS antenna is not also connected, mask this alarm in the Management -> Notifications pagee

### Log info associated with STL (Timing log ands Journal log)

- Refer to “1204-3D” in the SecureSync Option Card document: [..\SecureSync Option Card information.pdf](#)

### Summary of log info

- **Timing log** contains entries for burst info:

#### *Example entries*

Oct 4 07:32:27 Spectracom Spectracom: [system] 2017 277 07:32:36 000 STL Status: Total Burst:1 Strong Burst:0

Dec 1 12:02:16 Spectracom Spectracom: [system] 2017 335 12:02:16 000 AR stl0 has lost communication.

Dec 1 12:02:24 Spectracom Spectracom: [system] 2017 335 12:02:24 000 AR stl0 has established communication.

- **Journal log** contains user config changes to the STL configs

#### *Example entry*

Nov 27 20:35:20 Spectracom Spectracom: [webui] Changed STL Configuration for ASCII Reference 0 in slot 3 from STR (0) Configuration: Serial Number: EVK2-066 Latitude: 40.584330 Longitude: -74.243270 Altitude: 100.000000 EE axis: 100.000000 NN axis: 100.000000 UU axis: 50.000000 Geolocation mode: 1 Sensitivity level: 40 to STR (0) Conf: EVK2-066 0.708330 -1.295790 100.000000 100.000000 100.000000 50.000000 1 40

## GPS/GNSS (GNSS 0) input

### GPS/Glonass/QZSS SAASM GPS input reference- GPS Receiver operation /Mobile (Dynamic) mode operation/SAASM

#### Desire to add a GNSS receiver to the SecureSync/9400 in the field (after initial purchase)

- Requires hardware modification, and spfactory login to reconfigure the Options.
- Time server **does** have to be returned to factory for this hardware/software/ reconfiguration/ retrofit (even if the request is from one of our dealers).

#### Antenna jack/coax cable connection to the GNSS receiver

- GPS coax cable assembly P/N: CA01R-0NSB-80R6



As shown in Figure 19, measure the 5VDC voltage (the GPS receiver provides a nominal +5vdc to power the GPS antenna) across the rear panel antenna jack. Place the red probe of the meter on the center pin of the connector and place the black probe touching the threaded portion of the connector. There should be a nominal 4.8VDC to 4.9VDC present on this jack. If this voltage is NOT present, stop here and contact Spectracom Technical Support for additional assistance. If this 5VDC is not present, a problem internal to the SecureSync exists (the GPS receiver is not providing the +5VDC needed to power the GPS antenna). However, if the 5VDC is present, proceed to the next step.

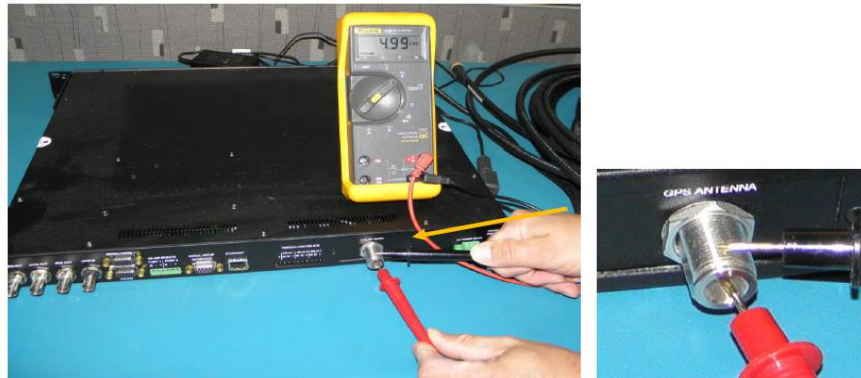


Figure 19: Verify 5vdc is present on the GPS antenna jack

#### Storage of receiver configurations, Backup/restore receiver configs Home/spectracom/config directory

| Config file name  | Configurations for: | Notes                                                          |
|-------------------|---------------------|----------------------------------------------------------------|
| <i>gpscf.conf</i> | GPS Receiver        | Interfaces -> GNSS 0 page<br>Rcvr mode, constellations, offset |

#### Circular Error Probability (CEP) for SecureSyncs/9400s

- Refer to SF case 124480

**Description:** CEP refers to the radius of a circle in which 50% of the values occur, i.e. if a CEP of 5 meters is quoted then 50% of horizontal point positions should be within 5 meters of the true position. The radius of the

95% is often quoted and the term R95 used. R95 is CEP with the radius of the 95% probability circle.

**Email from Dave L (4 Jan 18)** I did recognize the term CEP after reminding myself via Google.

**Circular Error Probability (CEP)**

CEP refers to the radius of a circle in which 50% of the values occur, i.e. if a CEP of 5 meters is quoted then 50% of horizontal point positions should be within 5 meters of the true position

The Spectracom Securesync uses the uBlox M8T GNSS Receiver. From the receiver data sheet:

Horizontal Position Accuracy with GPS is 2.5m.  
CEP, 50%, 24 hours static, -130dBm, > 6 SVs

[https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3\\_DataSheet\\_%28UBX-15025193%29.pdf](https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_%28UBX-15025193%29.pdf)

## Downloading/querying GNSS 0 data via CLI interface, .CSV file or REST API

### 1. Via .CSV file

- Python scripts to automate: refer to [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API - Postman and Python scripts\Python scripts\GNSS receiver](#)

### 2. Via REST API

- Refer to [REST API](#) section further below in this document

### 3. Via CLI interface

## GPS info (“GR\_” CLI commands)

- GR calls execute the GPS receiver’s protocol and determine 1PPS and time validity.
- Refer to the TSync family driver guide for a list of all GPS related API calls (1219 -5001-0050) in Arena
- Refer to Tim Tetreault’s “KITS cheat sheet” at: <..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet>

Note the same “GR\_” calls can be used with any Model receiver installed (RES-T, RES-SMT-GG as well as ublox). The Tsync drivers are upward and downward compatible with all of these receivers (the changes are for the ublox receiver are in the board’s firmware- so there was no need to change driver calls for the ublox receiver/.

Refer also to the GPS section of this document: [GPS input](#)

### Specific examples

**Note:** These are examples - additional calls may have since been added

```

spadmin@Spectracom ~ $ GR_Get
GR_GetAgpsServerState GR_GetDyn GR_GetMode GR_GetQualLog GR_GetUtc
GR_GetAlm GR_GetEphm GR_GetNumInst GR_GetRcvInfo GR_GetValidity
GR_GetAntenna GR_GetFixData GR_GetOffset GR_GetRefId
GR_GetConstSel GR_GetIono GR_GetParm GR_GetSatData
GR_GetCustom GR_GetMfrMdl GR_GetPosition GR_GetSurveyProg
spadmin@Spectracom ~ $ GR_Get

```

| API Call                        | Function                                                                                                                                                                                                                                |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TSYNC_GR_GetConstSel 0 0</b> | The command to switch between GPS and GLONASS on a TSync board (see notes further below). Only applicable to boards with GNSS receivers                                                                                                 |
| <b>TSYNC_GR_SetConstSel 0 0</b> | The command to switch between GPS and GLONASS on a TSync board (see notes further below). Only applicable to boards with GNSS receivers                                                                                                 |
| <b>TSync_GR_GetUtc 0 0</b>      | Should get UTC offset from the receiver.<br><b>Note:</b> this call may not be compatible with ublox receivers. With a uBlox installed in a SecureSync, this command responds with “RC_BAD_STATE”. May only work with Trimble receivers. |
| <b>TSYNC_GR_GetOffset 0 0</b>   | Get the GPS reference’s 1PPS input offset. Offset is in nanoseconds.<br><b>GR (0) Offset: 0</b>                                                                                                                                         |
| <b>TSYNC_GR_SetOffset 0 0</b>   | Set the GPS reference’s 1PPS input offset. Offset is in nanoseconds from -500 msec to +500 msec.                                                                                                                                        |
| <b>TSYNC_GR_GetValidity 0 0</b> | Get the GPS validity structure.<br><b>GR (0) Reference Validity:</b><br>Time: 1<br>1PPS: 1                                                                                                                                              |
| <b>TSYNC_GR_GetPosition 0 0</b> | Get the GPS position. Latitude and longitude are in radians. Altitude is in meters.<br><b>GR (0) Position:</b><br>Lat (deg): 43.083103<br>Lon (deg): -77.589073<br>Alt (m) : 172.880926                                                 |
| <b>TSYNC_GR_SetPosition 0 0</b> | Set the GPS position. Latitude and longitude are in radians. Altitude is in meters.                                                                                                                                                     |
| <b>TSYNC_GR_GetMode 0 0</b>     | Get the GPS receiver mode.                                                                                                                                                                                                              |
| <b>TSYNC_GR_SetMode 0 0</b>     | Set the GPS receiver mode.                                                                                                                                                                                                              |
| <b>TSYNC_GR_GetDynamics 0 0</b> | This API call is deprecated (use TSYNC_GR_GetMode instead)                                                                                                                                                                              |
| <b>TSYNC_GR_SetDynamics 0 0</b> | This API call is deprecated (use TSYNC_GR_SetMode instead)                                                                                                                                                                              |
| <b>TSYNC_GR_GetFixData 0 0</b>  | Get the GPS position fix data.                                                                                                                                                                                                          |





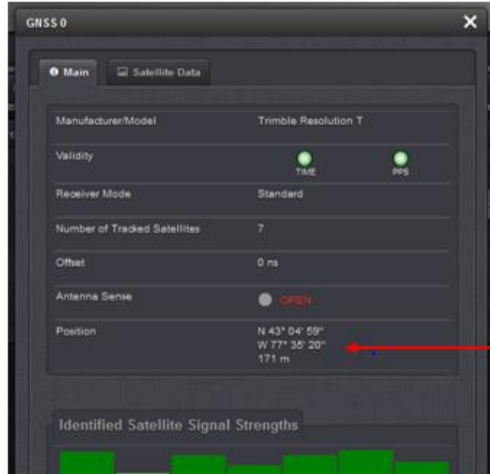
## \*\*Output GPS position information (Latitude, Longitude, altitude)

Q. Can you get GPS position information off of a SecureSync over the Ethernet port?

A. Yes! There are several ways to output position information:

### 1) Position is reported in the:

New web browser: Interfaces -> GNSS 0, Main tab



Classic interface web browser: Status -> Inputs -> GPS (as shown below):

| GPS INPUT STATUS   |                      |
|--------------------|----------------------|
| Manufacturer/Model | Trimble Resolution T |
| 1PPS Validity      | OK                   |
| Time Validity      | OK                   |
| Receiver Mode      | 1 Satellite          |
| Dynamic Mode       | Stationary           |
| GPS Longitude      | 077° 35' 20.674" W   |
| GPS Latitude       | 043° 04' 59.257" N   |
| GPS Altitude       | 169.918 m            |

### 2) Via CLI interface (Telnet or SSH session)

- Position info is also available via telnet or SSH connection (over Ethernet) using the `gpsloc` CLI command (as shown below):

```
[spadmin@Barrett_SideB ~]$ gpsloc
Position:
Lat N 43 4 59.120
Lon W 77 35 20.522
Alt 168 m
```

### 3) Via REST API interface

Per Ron Dries (29 July 2021) Position can be queried from the GNSS status Endpoint: [/Features/status/0000-0029-00.json](#)

### 4) Via SNMP Gets (v1/v2c or v3)

- Refer also to the SNMP documentation for SecureSync: [I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP](#) (such as the "SNMPGets-Sets" tab of the excel spreadsheet)

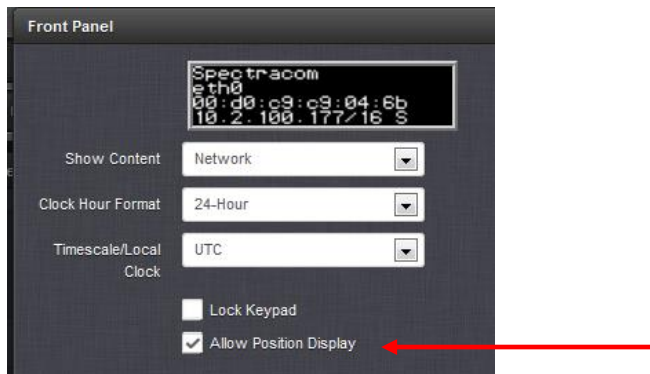
- Position info is also available via SNMP (over Ethernet) using particular OID numbers, as shown below:

| GPS/GNSS Receiver info                         |                                   |                 |                   |
|------------------------------------------------|-----------------------------------|-----------------|-------------------|
| Antenna Sense ("ssGpsRefAntennaState")         | .1.3.6.1.4.1.18837.3.2.2.2.1.1.17 | spec:SecSyncObj | ssGpsRefStatusObj |
| # Satellites being tracked ("ssGpsRefNumSats") | .1.3.6.1.4.1.18837.3.2.2.2.1.1.8  | spec:SecSyncMIB | spec:SecSyncObj   |
| GPS Time validity ("ssGpsRefTimeValid")        | .1.3.6.1.4.1.18837.3.2.2.2.1.1.4  | spec:SecSyncMIB | spec:SecSyncObj   |
| GPS 1PPS validity ("ssGpsRef1ppsValid")        | .1.3.6.1.4.1.18837.3.2.2.2.1.1.5  | spec:SecSyncMIB | spec:SecSyncObj   |
| GPS latitude ("GpsRefLatitude")                | .1.3.6.1.4.1.18837.3.2.2.2.1.1.13 | spec:SecSyncMIB | spec:SecSyncObj   |
| GPS longitude ("ssGpsRefLongitude")            | .1.3.6.1.4.1.18837.3.2.2.2.1.1.14 | spec:SecSyncMIB | spec:SecSyncObj   |
| GPS Altitude ("ssGpsRefAltitude")              | .1.3.6.1.4.1.18837.3.2.2.2.1.1.15 | spec:SecSyncMIB | spec:SecSyncObj   |

### 5) Via the Front panel LCD

- Though it's not "over Ethernet", it can also be displayed on the front panel LCD (unless it's been disabled in the web browser- for security concerns, the position display can be disabled via the web browser so that it can't be selected to be displayed using the front panel keypad)

**New web browser: Management -> Front panel page**



**Classic Interface: Setup -> Front panel page**



### 6) NMEA output Via ASCII RS-232 or RS-485 (requires a 1204-02 or 1204-04 ASCII output Option card be installed)

- **Model 1204-02** for RS-232 output
- **Model 1204-04** for RS-485 output
- Though it's not "over Ethernet", Position information can also be outputted via ASCII RS-485 and/or RS-232 data using NMEA data streams (GGA and RMC –NOT AVAILABLE with ZDA).
  - **Note:** This method requires one or more Model 1204-02 or 1204 ASCII Option Cards be installed.

## ICD-GPS-153c messages (Ground speed, heading)

- Per Paul Myers (23 Jan 17) "Force 22E ICD-GPS-153C messages provide ground speed and heading values"
- ICD-GPS-153 is apparently documentation for the DAGR:
- Refer to (ICD-GPS): <I:\Engineering\Specs and Standards\GPS>
- Refer also to SecureSync Option Card doc: <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>
- ASCII Output NMEA messages RMC, GGA, ZDA were designed for stationary applications because we don't populate all fields. The SecureSync otherwise is good for mobile applications.
- NRE needed to get needed values and transform/store and then add to ASCII Output message RMC
- Force 22E ICD-GPS-153C messages provide ground speed and heading values
- We would need to verify these values are correct and can be converted to values needed in RMC message which lacks them. And are in correct coordinate systems for RMC use.
- Message 5040 which we receive provides Ground speed
- Message 4 which we receive provides Attitude True Heading
- Check other GGA, RMC, ZDA for other issues.

### Example GGA message

\$GPGGA,123519.00,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,\*47

| GGA           | = | Global Positioning System Fix Data                                                                                                                                                                         |
|---------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 123519.00     | = | Fix taken at 12:35:19 UTC                                                                                                                                                                                  |
| 4807.038,N    | = | Latitude 48 deg 07.038' N                                                                                                                                                                                  |
| 01131.000,E   | = | Longitude 11 deg 31.000' E                                                                                                                                                                                 |
| 1             | = | Fix quality:<br>0 = Invalid<br>1 = GPS fix (SPS)<br>2 = DGPS fix<br>3 = PPS fix<br>4 = Real Time Kinematic<br>6 = estimated (dead reckoning) (2.3 feature)<br>7 = Manual input mode<br>8 = Simulation mode |
| 08            | = | Number of satellites being tracked                                                                                                                                                                         |
| 0.9           | = | Horizontal dilution of position                                                                                                                                                                            |
| 545.4,M       | = | Altitude, Meters, above mean sea level                                                                                                                                                                     |
| 46.9,M        | = | Height of geoid (mean sea level) above WGS84 ellipsoid                                                                                                                                                     |
| (empty field) | = | Time in seconds since last DGPS update                                                                                                                                                                     |
| (empty field) | = | DGPS station ID number                                                                                                                                                                                     |
| *47           | = | the checksum data, always begins with *                                                                                                                                                                    |

### "Fix Quality" value reported when SAASM receiver is keyed vs when its unkeyed

- Refer to SF case 163026

### Example RMC message:

\$GPRMC,123519.00,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W\*6A

| RMC         | = | Recommended Minimum sentence C          |
|-------------|---|-----------------------------------------|
| 123519.00   | = | Fix taken at 12:35:19 UTC               |
| A           | = | Status A=active or V=Void.              |
| 4807.038,N  | = | Latitude 48 deg 07.038' N               |
| 01131.000,E | = | Longitude 11 deg 31.000' E              |
| 022.4       | = | Speed over the ground in knots          |
| 084.4       | = | Track angle in degrees True             |
| 230394      | = | Date - 23rd of March 1994               |
| 003.1,W     | = | Magnetic Variation                      |
| *6A         | = | The checksum data, always begins with * |

**GPRMC and BBB-05 data steams: speed over ground and track angle info is not outputted (in at least software versions 5.5.0 and below)**

- Refer to Salesforce case 23871 for details <https://na28.salesforce.com/5001A00001D7db5>
- The Speed over ground and track angle fields are blank (this info is omitted from the data streams)

**Email from Paul Myers ( 9 Dec 16)** Hi Keith,

The reason why is that when the product was made with this feature it was stationary.

Since we have become mobile this is the first time someone has asked for this.

Can you make this a feature request to David Sohn.

**Email Keith sent to customer (13 Dec 16)** I checked with our software engineers with regards to these particular NEMA formats and their ability to provide mobile information. When they were initially incorporated into the SecureSync, they only needed to provide stationary information only (there was no Engineering requirement for them to be used in a mobile application). In order for them to be able to output speed and track data, information from each received data stream needs to be stored and processed, to output the mobile data, thereafter. This functionality has not yet been incorporated in the time servers, and is the reason the speed and track data is omitted in the data streams.

The SecureSync time servers are primarily used to provide very accurate timing. They aren't typically used for mobile data reporting, such as speed and track info.

I am forwarding your request, to have this additional information provided in the data streams, over to our Product Manager for his consideration of having our Engineering team add this capability via a future SecureSync software update. I am flagging your record in our service database to let you know if he decides to incorporate this capability and if so, when it has been implemented!

Please let me know if you have any other questions or need anything else from us in the mean-time!!!

---

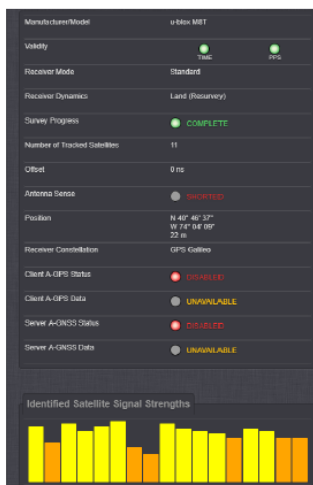
## GPS reception issues/GPS Jamming

- For GPS reception issues, refer to the SecureSync or NetClock GPS reception tech note: I:\Customer Service\GPS\GPS reception Ap Notes
- For information/suggestions on eliminating GPS jamming, refer to "Jamming" in the custserviceassistance doc

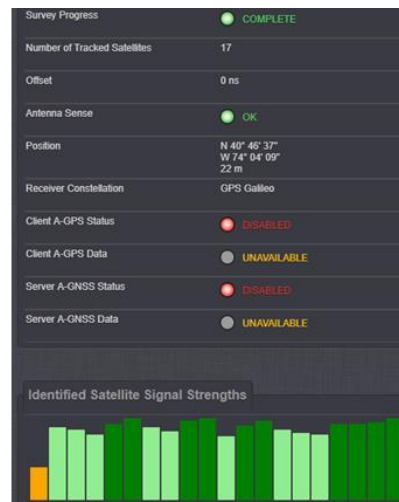
## Water leaking into cable (Antenna Sense=Short, but receiver still tracking satellites)

- Refer to Salesforce Case 230174
- GPS signal strengths may be much lower than normal
- Check for water/condensation inside the cabling (such as from the antenna to the surge suppressor)

Water leaking into cable



After fixing water leak



---

## Time it takes for NTP to sync after power-up:

Refer to "Time after initial boot-up for NTP to sync as Stratum 1" (such as in a mobile environment)

---

## GPS 1024 Week roll-over issue due to number of bits in the message (GPS Epoch every 20 years)

- For more info, refer to sites such as: <http://www.colorado.edu/geography/gcraft/notes/gps/gpseow.htm>

**Note:** The next 1024 week rollover occurs in ~~7 April, 2019~~ **April 2039**

- **On our website:** <https://spectracom.com/resources/blog/lisa-perdue/2017/gps-2019-week-rollover-what-you-need-know>

**Email from Dave L (12 Feb 18)** The Receiver Year Rollover will occur in April 2049. None of the receivers used in the SecureSync product are affected by the year 2019 GPS week rollover issue.

Here is some more information from our website:

<https://spectracom.com/resources/blog/lisa-perdue/2017/gps-2019-week-rollover-what-you-need-know>

Q I have been made aware of an issue with another manufacturer of GPS Clocks and although not one we use it prompts me to ask the same question to all our clock suppliers.

Apparently, there are several scenarios when a GPS clock can roll over due to “a limited number of bits in the satellite message”. A roll over in a Gorky unit is believed to have failed in the past and there will be a major roll over in 2019.

Could you confirm that a limited number of bits in the satellite message will not cause the Spectracom 9383 units we have in service to fail in any way?

**A Email from Paul Myers (22 Jul 16)** “This is an end of epoch issue a 20 year period of GPS weeks which rolls over in a counter which can't go beyond the number 1024.”

---

### Testing/certification of our GPS receivers

**Email Dave L sent to a customer (2 Dec 16)** I have confirmed that none of the receivers used in the SecureSync product are affected by the year 2019 GPS week rollover issue.

**Earlier email (don't recall from whom or when):** Our Engineering department had done a quick test with a Rollover scenario and our SecureSync continued to function normally and without any problems.

As such, we are able to inform you with a high level of confidence that our SecureSync shall NOT be affected by the Rollover problem.

However, as informed earlier – we shall still be doing a more elaborate series of tests the first week of March 2015 after which we shall send you our test reports for onward submission to OKI for their records.

We hope the above confirmation is to your satisfaction.

### Resolution-T GPS receivers (9183, 9283, 9383, earlier 9400s and earlier SecureSyncs)

Q. From Dick Fox to Dave Sohn: Do you know what is meant by GPS week counter roll over problem? Is this a known issue with other GPS receiver? Does the Res-T receiver have this issue?

**A Reply from Dave Sohn (2/21/13 KW)** The GPS week rollover issue would be caused as the GPS week counter rolls over back to zero, indicating another GPS epoch. Some receivers may have issues responding to this, causing errant behavior on the year, day of year reported. The receiver we utilize in SecureSync does not have a GPS week rollover issue

**Note about Dave's response above:** Dave asked Lisa Perdue to test a Res-T GPS receiver for the week roll over issue, using a GSG Simulator. The testing worked just fine. She did not experience any roll over issues.

---

### GPS/GNSS receiver and antenna (such as Model 8230) is “receive-only” (it doesn't transmit)

- For documentation indicating the GPS/GNSS receiver is receive only, refer to:
  - “GPS antennas are Receive-only” in <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>
  - The “Model-specific” document: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\GPS-GNSS\GPS is receive-only>

---

### Storage of Almanac and Ephemeris data/A-GPS server license

Q Our customer would like to know the condition of the cold start and warm start.

1. Does the CF card be stored Almanac and Ephemeris orbit information?
2. Does the Lithium ion battery be stored Almanac and Ephemeris orbit information?
3. If yes, expired period is same as in general?

- Almanac: several days
- Ephemeris: 4 hours

We could find this description in User's manual. "Rinex files (ephemeris data) must be updated no later than every 2 hours, because the ephemeris data is valid for 4 hours."

**A Reply from Ron Dries to Josh Goh (24 Jan 2020)** The ublox m8t receiver stores Almanac and Ephemeris data and handles updating it as necessary. If they issue a cold restart, then the receiver will clear out both the Almanac and Ephemeris. Otherwise it will keep the data, and then update it if necessary.

The Almanac and Ephemeris data can be saved to the CF card only if using the A-GPS server licensed option. There is configuration required from the user on when to have the files created. Our online manual describes this functionality in detail if they are interested in using it: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/AGPS.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/AGPS.htm)

## GPS/GNSS Receiver Models

### Determining which Model receiver is installed and its current firmware version

Email from Keith The Model of the GNSS receiver and its installed version is reported about half way down, in the **Tools -> Upgrade/Backup** page of the browser (under System Configuration), as shown below





---

## Commercial GPS/GNSS receivers

### uBlox M8T, Trimble Res-SMT-GG and Trimble Res-T

Resurvey/Need to manually delete position in Stationary Mode in Res-SMT-GG and uBlox receivers (not applicable to Res-T receivers)

| GNSS Receiver      | Receiver firmware version                                                                                   | Resurvey requirements                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| uBlox M8T          | All uBlox firmware versions                                                                                 | A) <b>Update versions 5.4.5 (and above):</b> Spectracom software now causes uBlox receiver to automatically re-survey upon each unit power-up.<br>B) <b>Update versions 5.4.4 (and below):</b> Software versions prior to versions 5.4.4 need position manually cleared by a user, if receiver is relocated after initial sync to GPS                                                     |
| Trimble Res-SMT-GG | Trimble firmware v1.9 and above (v1.8 and below automatically resurvey upon sensing receiver was relocated) | A) <b>Update versions 5.7.0 and above:</b> Spectracom software now causes Res-SMT-GG receiver to automatically re-survey upon each unit power-up.<br>B) <b>Update versions 5.6.0 and below</b> (and receiver having v1.0.9 firmware installed): A user must manually delete the receiver's position with firmware 1.0.9 installed, and if receiver is relocated after initial sync to GPS |
| Trimble Res-T      | N/A                                                                                                         | N/A                                                                                                                                                                                                                                                                                                                                                                                       |

---

#### uBlox log entries in Timing log

- Refer to the "uBlox receiver" section in the custassist doc: <..\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>

---

#### \*\*Desire to Blacklist (Mask/Unmask) a Satellite from being received by a Trimble RES-SMT-GG receiver

- Refer to Salesforce case 179110
- Refer to the sub-section "**Desire to Blacklist (Mask/Unmask) as satellite:**" (in the "Trimble RES-SMT-GG" section) of the cust assist tech note: <..\CustomerServiceAssistance.pdf>

## u-blox Model M8T receivers

Refer also to M8T info in: [:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf](file:///C:/Customer%20Service/1-Cust%20Assist%20documents/Customerserviceassistance.pdf)

- This is a 72 channel GNSS receiver
- Software support for this receiver added in v5.4.0/5.4.1 (~Mar 2016)
- Initial M8T receiver firmware version when we started shipping them: version 2.01

|               |            |          |
|---------------|------------|----------|
| GNSS Receiver | u-blox M8T | SW V2.01 |
|---------------|------------|----------|

- Cut-in of ublox receiver for SecureSync/9400s: ~18 March, 2016 (S/N 11719, per Jill)
- (refer to ECO-000781 [https://app.bom.com/changes/detail-summary?change\\_id=2385971714](https://app.bom.com/changes/detail-summary?change_id=2385971714))
  - **Description:** Replace Trimble receiver, MP30R-0GNS-0001, with U-BLOX GNSS receiver, 1240-0000-F001, in SecureSyncs.
- Refer to additional info on the M8T receiver in [.\CustomerServiceAssistance.pdf](file:///C:/CustomerServiceAssistance.pdf) (search it for “M8T”)

### Sensitivity/Gain for the ublox M8T receiver

|                            | ublox receiver min sensitivity |                  | Res-SMT-GG sensitivity (for comparison) | Notes                                                             |
|----------------------------|--------------------------------|------------------|-----------------------------------------|-------------------------------------------------------------------|
|                            | (GPS and Glonass)              | (GPS and Beidou) |                                         |                                                                   |
| <b>Acquisition</b>         | -148 dBm                       | -148 dBm         | -155 dBm                                |                                                                   |
| <b>Tracking/Navigation</b> | -167 dBm                       | -165 dBm         | -160 dBm                                | -136 dBm (-160dBW) at surface of the Earth. (Need min 16 dB gain) |
| <b>Reacquisition</b>       | -160 dBm                       | -160 dBm         |                                         |                                                                   |

### dB Gain

The recommended minimum to recommended maximum dB gain (Antenna/GPS preamp dB gains, minus the antenna cable loss) at the input to the GPS receiver is 16dB. This can also be stated as the following:

The GPS signal at the surface of the earth is -136dBm. The minimum sensitivity for the GPS receiver in the SecureSyncs/TSync boards which have a ublox receiver installed is **-148 dBm**. There has to be enough antenna gain (and inline GPS amps, if needed) to account for the antenna cable loss, for the signal to be at least -145 dBm. The antenna cable loss for Belden RF400 or Time Microwave LMR-400 cable is about 5.5 dB loss/100 feet of cable.

**Recommended gain at the GPS receiver (per the receiver manufacturer): 5 dB to 20dB gain**

The NEO-M8T includes a SAW filter and an additional LNA and is suitable for use with both passive<sup>13</sup> and active<sup>14</sup> antennas. The LEA-M8T includes a SAW filter and is suitable for use with active antennas and antenna distribution systems. Within the recommended range below, lower overall gain can improve immunity to interference in most situations; higher gain offers slightly better sensitivity.

Antenna Type

Active Antenna Recommendations

|                      |                         |
|----------------------|-------------------------|
| Minimum gain         | 5 dB (at module input)  |
| Maximum gain         | 20 dB (at module input) |
| Maximum noise figure | 1.5 dB                  |

---

## ublox M8T current specs (5vdc to antenna)

### The antenna's protect/detect circuit will:

- **short circuit** at around 100 mA.
- **An open circuit** is determined if the antenna current falls below approximately **6 mA**.

---

## GPS-only is still the standard (factory default) configuration ?

“**SS-Opt-GNS**” (<https://na28.salesforce.com/01tC0000003IGr1?srPos=0&srKp=01t>) also adds **Glonass, BeiDou** and **QZSS**

- ? **Galileo constellation**: the ublox M8T receiver is hardware compatible with the Galileo constellation, but a receiver firmware update (beyond versions 2.01) for the Receiver/ and software update for SecureSync will be needed- expected around Q4-2016)

## Factory update/Field upgrade, Desire to swap-out a Trimble receiver for a uBlox receiver

- for SecureSyncs/NetClocks purchased prior to Jun 2016, when the ublox receivers were cut-in . Cut-in S/N for ublox was 11719):

### A) Factory upgrade of Trimble receiver (Res-T/Res-SMT-GG) to a uBlox receiver

- Repair Price Books in Salesforce shows we offer a factory upgrade of SecureSyncs to a uBlox receiver for \$720.00 (Our P/N “UG-REC-UBLOX-SS” at <https://orolia.my.salesforce.com/01t0h000004kas2>)

**Email from Dave Lorah (11 May 2020)** Hi Nick, Keith,

We do have a price for upgrading to a U-Blox which also includes the front panel update mod for fan control and a CF card if needed. The price is \$800.

### B) Field upgrade of Trimble receiver (Res-T/Res-SMT-GG) to Ublox receiver

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\GPS-GNSS\convert RES-SMT-GG to ublox receiver>

#### This process requires:

1. The unit be returned to the factory for an EPROM upgrade.
2. Software to be at least versions 5.4.0 or above.

Q I would like to know if it is possible to field upgrade my SecureSync with a Trimble RES-SMT GG GNSS unit to a newer u-blox M8-T GNSS unit; if this is possible, what is the cost of the u-blox receiver.

**A Keith's response to Nick Haddad (24 Jan 2020) so that he could respond to question above.**

I do not believe we currently offer a field-update package for swapping out a SecureSyncs Trimble receiver with a uBlox receiver. If it was just a matter of swapping the two receivers, this would be easy with just following standard ESD protection practices. However, there is an EPROM reprogramming also required, as well. This usually requires the SecureSync be returned to the factory.

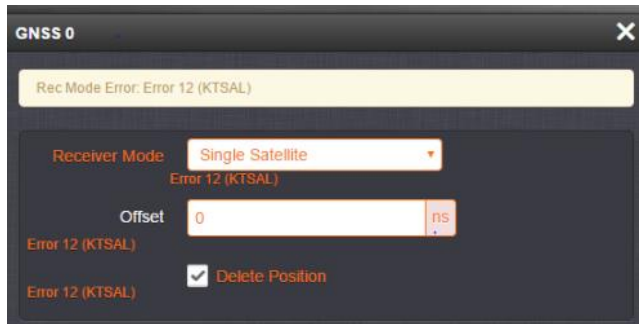
We once sent a patch file to one of our international dealers (as I recall) some time ago, which allowed the reprogramming of the EPROM in the field. But I haven't heard that we have agreed to offer this patch and a new uBlox receiver to customers for a field update. If we were willing to offer this as a field update, we would need to establish the purchase price.

Repair Price Books in Salesforce shows we offer a factory upgrade of SecureSyncs to a uBlox receiver for \$720.00 (Our P/N “UG-REC-UBLOX-SS” at <https://orolia.my.salesforce.com/01t0h000004kas2>)

If we don't offer the receiver upgrade as available for fielded units, I believe the cost above is what you need to inform the customer (Dave/Scott can you confirm the above info/my understanding, for Nick? Thanks!!!

---

**“Rec Mode Error: Error 12 (KTSAL) message displayed with a ublox receiver installed (S/Ns 11719 and above)**



- Make sure main software has not been downgraded to any software version earlier than version 5.4.0 (version 5.4.0 is the minimum version that supports communications with a ublox receiver)

---

**“GPS0 UBX Message receive Checksum Error”/ “GPS0 UBX Message receive buffer overflow**

**A) Both error messages above asserted**

- Refer to Salesforce Case 274882

**Report from customer** We had a weird problem that we are unable to reproduce. We booted up the SecureSync 1200 (with a u-blox 8) connected to a GPS antenna and it started getting two error messages:

046 GPS0 UBX Message receive Checksum Error  
031 GPS0 UBX Message receive buffer overflow

The errors persisted through one hardware reboot and did not through a second.

**B) Just “GPS0 UBX Message receive Checksum Error” asserted**

- Refer to Salesforce Case 232034

**Email from Ron Dries (8 May 2020)** Looking in the timing.log file there are a lot of checksum error messages:

May 7 11:38:50 Spectracom Spectracom: [system] 2020 128 11:38:50 046 GPS0 UBX Message receive Checksum Error  
May 7 11:38:53 Spectracom Spectracom: [system] 2020 128 11:38:53 046 GPS0 UBX Message receive Checksum Error  
May 7 11:38:57 Spectracom Spectracom: [system] 2020 128 11:38:56 046 GPS0 UBX Message receive Checksum Error  
May 7 11:38:59 Spectracom Spectracom: [system] 2020 128 11:38:59 046 GPS0 UBX Message receive Checksum Error  
May 7 11:39:00 Spectracom Spectracom: [system] 2020 128 11:39:00 046 GPS0 UBX Message receive Checksum Error

This indicates to me that there is communication issues between KTS and the GPS receiver, but I don't see any indications of other communication issues so KTS is still functioning correctly.

My feeling is that it is something with the receiver but I think we will need to RMA it to diagnose what happened for sure.

**Update** (2 Aug 2021) for RMA 232034, Repair team found faulty/replaced GNSS receiver

---

**Difference between Trimble and ublox receivers regarding Standard mode (ublox doesn't re-survey)**

- Update version 5.4.5 is implementing a software change that causes the ublox receiver to perform a new survey if it's relocated after completing a survey in Standard/Stationary mode - alleviating the need to manually delete the position.

**Need to manually delete position after relocating receiver to perform a new GPS survey (applicable to versions 5.4.1 and below) 5.4.5 and above default to resurvey upon each boot-up.**

- Update to software version 5.4.5 or above to alleviate the need to manually delete position once ublox receiver has synced in Stationary mode and subsequently relocated.
- By factory default, versions 5.4.5 (and above) causes GPS resurvey after each system power-up. (a user can reconfigure the receiver dynamics code in *Interfaces* -> *GNSS 0* page to not resurvey, if desired)

*Per Paul M (9/7/2016)*

**U-Blox Resurvey on Reboot**

- Resurvey's on reboot by default
- User can select NO resurvey option by adjusting Dynamic value
- Standard Land (Resurvey)
- If the user selects this mode, every reboot the U-Blox receiver ONLY re-survey's.
- This is default product behavior.
- Standard Stationary (No Resurvey)
- If user selects dynamic value of stationary, then NO resurvey is performed on reboot.
- This is to avoid dissatisfying customers who don't want this.

**Email from Dave Sohn to Derek (3 Jun 16)**

Here was a statement I put together for service on this:

One of the characteristics of the new u-blox receiver is that it does not automatically "resurvey" its position in standard (stationary) mode if the unit is relocated. Stationary mode provides some improved timing stability, operation down to a single satellite, and is able to employ a T-RAIM algorithm that can exclude satellite signal measurements that fall outside expected values. Normally, this behavior is not problematic, however when pre-staging deployments or redeploying systems, the system will survey at the staged location and won't resurvey again at the deployed location, which will prevent the system from synchronizing. The system may show tracked satellites, but will not synchronize to the constellation.

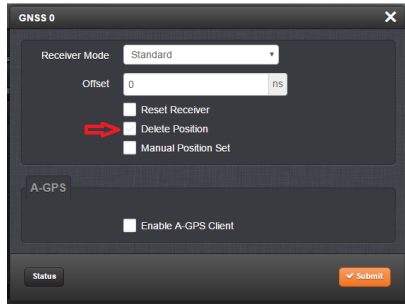
The Spectracom factory has always cleared location (and history) on all SecureSyncs before shipping them to any of our customers, so delivered units will always perform a survey on location.

There are two options to minimize any noticeable impact on systems due to staging prior to a move to final install site

- 1) Change the staging process to perform a "Delete Position" as part of the system power down (details below).
- 2) As part of the configuration done during staging, enable mobile mode, which does not perform the survey process. This will not have any appreciable effect on 1PPS (or 10MHz) accuracy. We only saw a difference of 3 ns between the 1 sigma 1PPS synchronization accuracy over 24 hours between the two modes.

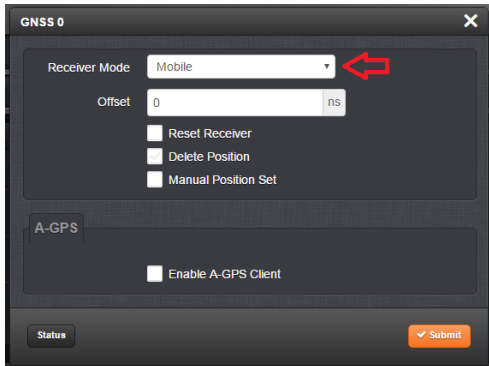
**To clear position:**

1. Launch a web browser and load the web user interface of the unit
2. Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)
3. On the “Main” tab, click the “Edit” button
4. Check the “Delete Position” selection and click the “Submit” button
5. The survey will automatically restart
6. Shut down the unit prior to survey completion (~33 minutes)



**To enable mobile mode:**

1. Launch a web browser and load the web user interface of the unit
2. Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)
3. On the “Main” tab, click the “Edit” button
4. Change the “Receiver Mode” selection to “Mobile” and click the “Submit” button



---

## Trimble Res-SMT-GG GNSS receivers

- Replaced Trimble Res-T GPS receivers (then replaced by ublox M8T receivers)
  - **Our P/N:** MP30R-0GNS-0001
  - **Trimble P/N:** 99974-00

### Receiver Cut-in info/ Software support

**SecureSync:** Software versions 5.0.0 and above support the RES-SMT-GG (and RES-T) receivers.

- Earlier firmware versions need to be updated to v5.0.0 to be able to work with a RES-SMT-GG receiver (ECN 3244, June 2013)

**SecureSync/9400 Cut-in info** (SecureSync/NetClock 9400s: Switching from Trimble Res-T to Res-SMT receivers)

- Cut-in ECN to support RES-SMT-GG receiver in SecureSyncs: ECN 3228, 7 Nov 2013 (ECN closed)
- Cut-in ECN to support **RES-SMT-GG receiver in NetClock 9483/9489:** ECN 3265, 7 Nov 2013 (ECN closed)

**Note:** I believe we actually started **shipping** SecureSyncs/NetClock 9400s **with Res-SMT-GG** receivers **~2 Apr 2014 (~S/N 5950).**

**Note:** Since this is only an estimated date/serial number for the cut-in. it's recommended to verify the receiver Model via the **Interfaces** -> **GNSS 0** page of the browser to be certain, if the unit is near this Serial Number.

### Later change from Trimble RES-SMT-GG to ublox M8T receivers

- Ublox M8T receivers cut-in was S/N 11719 (9 Jun 16- this was a Model 9489)

---

### Temporary Deviation 000047 for shipping Res-T receivers (instead of Res-SMT receivers) to use up stock

- This deviation was implemented after we had started shipping Res-SMT-GG receivers in SecureSync/9400s
- Deviation 000047 (May 2015) to ship Res-T in place of Res-SMT-GGs (except for Harris and Skylight)
  - Refer to : [https://app.bom.com/changes/detail-summary?change\\_id=2385096515](https://app.bom.com/changes/detail-summary?change_id=2385096515)

### Desire to upgrade Trimble receiver to Ublox receiver

- Refer to the “**ublox receiver**” info further above

---

## Res-SMT-GG firmware versions and known issues

### A) Res-SMT-GG receiver versions

- Refer also to: [Software release dates.xlsx](#)
  - v1.10 (bad satellite PRN27 fix)
  - Applied in update [version 5.8.6](#) (Oct 2019)
  - Refer to JIRA ticket SSS-585 (Trimble SMT-GG v1.10 Release Notes below:

#### Change Description

1. Update libraries for tracking and navigation to address the issue of satellites being dropped for 1 to 2 seconds. The issue was caused by the tracking loop losing lock if there were too many consecutive digital "ones" in the satellite data and being mistaken for jamming.

The resolution was to increase the interference detection observation time so that any properly formatted GPS frame will not cause the interference detector to trigger. This still maintains the ability to detect true jamming conditions, where there is no framing information contained in the transmitted signal.

2. During the time period of Oct 7, 2018 the PPS output on some units were exhibiting 1 millisecond PPS errors. This offset would continue for a couple of seconds, then return to the correct phase, only to repeat the issue again in about 30 seconds. These "bursts" of PPS error would continue for 60 to 300 seconds. The PPS then returned to normal operation.

In looking at the almanac data gathered from another, independent receiver, anomalies were observed in the data being transmitted in the almanac information for PRN27 which persisted until Oct 11, 2018. These anomalies contained different PRN 27 almanac information being transmitted from different satellites.

The methodology of the marking of the health, while allowed by the ICD, was slightly irregular. The almanac data containing orbital parameters being transmitted by the satellites for PRN27 included a very large error in the clock offset for the satellite.

The module contains code for a false correlation locking routine that would disqualify a satellite if there was a large discrepancy between the orbital parameters, but it failed to take into account a false lock due to a large clock discrepancy.

The correlation locking routine was modified to correct that shortcoming by forcing use of the ephemeris parameters immediately upon detection of the error. This causes PRN27 to be reacquired, with proper phase and data correlation so that there is no longer a 1 millisecond error for that satellite.

3. Added robustness on system time correction and improved the management for the almanac updates.

- **1.09 (1.9)** applied in update [version 5.4.5](#)
- **1.08 (1.8)** applied in update [version 5.3.0](#)
- **1.07 (1.7)** applied in update [version 5.1.7](#).
- **1.06 (1.6)** I believe this is the first version we have used since we started shipping Res-SMT receivers (Res-SMT-GG receiver started shipping ~2 Apr 2014 while we were shipping v5.1.3)

#### B) Known issues with RES-SMT-GG receivers

##### **\*\* (Oct, 2016, Sept 2021) 1PPS timing glitch due to a minor math issue relating to the GPS week number (associated with at least versions 1.6 thru 1.9)**

- Refer to "06-02-1024-02-ACU\_ResSMTGG.UTC-PPS.pdf: I:\Customer Service\GPS\GPS receivers\Res-SMT-GG receiver
- Refer to "known firmware issues with RES-SMT-GG receivers" in the RES-SMT-GG section of the custserviceassistance document.
- Next event not expected to be seen aboing until Sept, 2021.
- At least Trimble firmware versions 1.6 through 1.9 are affected (not known at this time if Trimble intends to fix this).

##### **\*\* (Sept 2016) RES-SMT-GG receiver firmware version 1.09 (1.9) doesn't resurvey/resync after being relocated**

- Refer to the Res-SMT-GG receiver section of the custserviceassistance doc for details
- Have to delete GPS position after GPS Time data will be valid (green) but GPS PPS will remain not valid (red) unit position is deleted in the Interfaces -> GNSS 0 page of the browser.relocating receiver before it will go into sync (even though its tracking satellites just fine)

##### **\*\* (June 2015) RES-SMT-GG receiver firmware versions 1.07 (1.7) and 1.06 (1.6)**

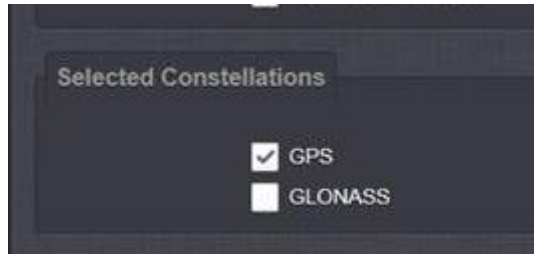
**Issues fixed in firmware version 1.0.8 (1.8), which was implemented in SecureSync software update version 5.3.0)**

#### A) Loss of GPS reception for just one or a couple of seconds (with Glonass license installed)

- Temporary work-around until firmware version 1.08 ("1.8") can be applied is to disable Glonass satellites and leave just GPS enabled.



- Glonass can be disabled in the **Interfaces** -> **GNSS 0** page of the newer browser (as shown below):



**Email from Paul Myers (30 June 15)** Results in testing thus far show the RES-SMT-GG v1.08 improves PPS Stability when using GPS+GLO. Also our observation of Qualification Logs on SecureSync's shows good tracking performance with multiple SecureSync's showing no drops to 0 satellites when running v1.08, while a control unit running v1.07 does show a few drops to 0 satellites for 1-2 sec.

Tim T has been doing board testing with 1.08 and we should check to see if he is seeing any 0 satellites log entries.

V1.08 is in the SecureSync 5.3.0 release.

## B) Poor 1PPS accuracy/performance (high phase errors) when Glonass is enabled

- For SecureSyncs, this only applies with units that have Glonass license installed and have Glonass enabled
- Short term fix (as of 30 Jun 2015) until a field update for 1.0.8 is available is to disable Glonass, if possible. Or the GNSS receiver can be returned to us for update to 1.0.8 if Glonass reception is necessary.
- SecureSync Software update version 5.3.0 implemented firmware version 1.0.8 (1.8) update for the **Res-SMT-GG receiver**.

## C) (Sept 2014) RES-SMT-GG receiver firmware version 1.0.6

**Note:** All of the RES-SMT-GG receiver issues listed below were resolved with the RES-SMT-GG Receiver firmware upgrade version **1.0.7**, implemented with the **version 5.1.7** and above software update.

### 1. Potential for RES-SMT-GG receiver to cause time jumps (several seconds) in SecureSyncs/9400s (with software versions 5.1.3 or 5.1.4 installed)

**Potential Issue:** Res-SMT-GG receivers can potentially start to output the wrong number of seconds of UTC offset for a period of time, resulting in System Time jumping by the error in this value, when the board is synced to GPS. The GNSS receiver automatically corrects the time with the next ephemeris download (within 12.5 minutes).

- Can affect SecureSync or 9400 series NetClocks with a Res-SMT-GG receiver installed (see cut-in information directly above) when firmware version 1.0.6 is installed in the receiver, while synced to GPS.
- Can occur in software versions prior to version 5.1.5 (version 5.1.5 added a work-around that prevent the System Time from changing, if the RES-SMT receiver happens to output an erroneous timescale offset value).
- Crabel Capital observed a 12 second time jump occur on a SecureSync for about 6 minutes. Then it automatically corrected (refer to Salesforce case 15783)
- Version 5.1.5 update added a mask to our software to prevent this issue from being observed.
- Version 5.1.7 update made available the version 1.0.7 firmware update to RES-SMT-GG receiver to fix this issue.

### 2. 1PPS jump of a few hundred milliseconds

- Refer to Mantis case 2935:

- Summary: 1PPS Jump in RES-SMT-GG might be caused by a position change in receiver calculations.
- Description: The unexpected 1PPS jump to a few hundred msec off of the GPS 1PPS 'might' be caused by an intermittent error in the position calculation causing the GNSS receiver to incorrectly adjust 1PPS.

### 3. Erratic leap second warning asserted

- Reportedly fixed with the Res-SMT-GG version 1.0.7 firmware update, being made available in the SecureSync version 5.1.7 update (Nov, 2014)
- Note: This erroneous leap second being scheduled is not likely to be applied to the system. So it's highly unlikely to affect operation of the SecureSync. With versions 5.1.7 and below, and as long as the System time scale is still set to UTC, the leap second is only applied if the amount of leap second to be applied is "+1" or "-1".
- The erroneous scheduled leap second from version 1.06 receiver firmware is instead setting this to a much higher value than 1, such as +6 or +72 for examples. Even though the leap second is scheduled, this bad data won't result in a leap second correction occurring (unless its erroneously set to a 1). And the receiver is scheduling out the leap second, long after the one scheduled for June 2015. So it will be cancelled out by the real leap second.
- However, if the system is in GPS or TAI timescale with version 5.1.7 or below installed, the leap second will take if scheduled before June 2015. The Jan 2015 release is adding additional protection that the system will only accept a 1 second change no matter what the system timescale is set to.
- The leap second scheduled for June 2015 will override/delete any erroneous scheduled leap seconds. Or a user can manually delete with the browser, if they wish/.

**Per Dave Sohn (8 Jan 15, referring to v5.1.7)** Better protections for this are already in place and will be included in the next release (referring to 5.2.0 release in Jan 2015). However, despite the reporting of the leap second, a leap second of greater than one second will not occur if the unit is operating in a UTC timescale, which is the default for SecureSync. Also, a leap second can be removed from the system, if present, by using the delete mechanism from the Edit Leap Second window on the Management -> Time Management page of the browser.

### 4. GPS goes "not valid" every other second (if no other references, goes into Holdover every other second)

- Likely (but not confirmed) fixed with the Res-SMT-GG version 1.0.7 firmware update, being made available in the SecureSync version 5.1.7 update (Nov, 2014). Emmanuel observed this same issue with an Epsilon clock with a Res-SMT-GG receiver installed.

### 5. Cold reset of SecureSync with RES-SMT-GG results in return to last saved GNSS Receiver Mode

- Refer to Mantis case 2932 <http://10.30.1.21/mantis/view.php?id=2932>
- Summary: A Cold Reset deletes all RAM data and acts like a power cycle of the RES-SMT-GG (or RES-T).

---

## D) After GPS survey has completed, changing position results in SecureSync with invalid 1PPS and failure to resurvey

- Refer to Mantis case 2935 (<http://10.30.1.21/mantis/view.php?id=2935>)
- Reported Nov, 2014
- Summary: During a test to try to explain the unexpected 1PPS jump to a few hundred msec off of the GPS 1PPS 'might' be caused by an intermittent error in the position calculation causing the GNSS receiver to incorrectly adjust 1PPS we found that the SecureSync would experience three errors

---

## GPS-Glonass-BEIDOU-QZSS-Galileo satellite constellation / number of satellites being tracked

**Note:** Glonass and/or QZSS capability requires both a GNSS receiver (such as either RES-SMT-GG or ublox) and purchased Glonass license file be installed. Galileo requires a ublox receiver with version 3.0.1 or higher firmware installed (I don't believe Galileo is available with RES-SMT-GG receiver).

**Note:** update version 5.7.0 (Jun 2017) alleviates the need to purchase the multi-GNSS license if its desired to add additional constellations beyond just GPS. Once a unit has been updated to 5.7.0 or above, the unit has the ability to enable GPS and other satellite constellations (units with just GPS before updating will just have GPS enabled after updating. But they can then go in and enable other constellations if desired).

**License files** (there is one for SecureSync and one for NetClock Models 9483/9489)

- **For SecureSync ("SS Opt-GNS") Refer to:**  
<https://na28.salesforce.com/01tC0000003IGr1?srPos=9&srKp=01t>
- **For NetClock 9400s ("NC Opt-GNS") Refer to:**  
<https://na28.salesforce.com/01tC00000043YtE?srPos=7&srKp=01t>

### Using a Model 8228 window-mount antenna with a GNSS receiver having multi-constellation support

- The Model 8228 antenna is a GPS constellation-only antenna.
- Can still be used to track GPS satellites, but won't allow the receiver to track any other constellation besides GPS

Q Does 8228 indoor antenna support SS-OPT-GNS?

**A Keith's response (5 Oct 17):** The Model 8228 window-mount antenna is a GPS constellation-only antenna. Since it can only receive GPS signals (it can't receive Glonass, Galileo, etc) a GNSS receiver in the SecureSync which is connected to this antenna will only be able to track GPS satellites. So it can't be used with a SecureSync, if it's desired for the SecureSync to be able to track satellites beyond just GPS satellites.

## A) Galileo

### 1. For SecureSync ("SS Opt-GNS")

- **Refer to:** <https://na28.salesforce.com/01tC0000003IGr1?srPos=9&srKp=01t>

### 2. For NetClock 9400s ("NC-Opt-GNS")

- **Refer to:** <https://na28.salesforce.com/01tC00000043YtE?srPos=7&srKp=01t>
- Galileo availability started with ublox receivers having firmware version 3.0.1 installed (~Dec, 2016).
  - Galileo was not initially available in the first version installed (v2.3.0) when we started using ublox receivers.
  - Galileo not available with Trimble Res-T or RES-SMT-GG receiver installed in time server.
  - Galileo only displayed if purchased Galileo license file is installed.

### Summary of Galileo support

| Receiver           | Galileo available? | Requirements                                                                     |
|--------------------|--------------------|----------------------------------------------------------------------------------|
| uBlox M8T          | Yes                | 1. Software vupdate v5.7.0 or above<br>2. uBlox firmware version 3.0.1 or higher |
| Trimble Res-SMT-GG | No                 | N/A – Galileo Not available                                                      |
| Trimble Res-T      | No                 | N/A – Galileo Not available                                                      |

## B) Glonass

- For SecureSync (“SS Opt-GNS”) Refer to:  
<https://na28.salesforce.com/01tC0000003IGr1?srPos=9&srKp=01t>
- For NetClock 9400s (“NC Opt-GNS”) Refer to:  
<https://na28.salesforce.com/01tC00000043YtE?srPos=7&srKp=01t>
  - Glonass capability was added in software update version 5.1.5 (I believe)
  - Glonass not available with Trimble Res-T receiver or with software versions 5.1.4? and below
  - Glonass only displayed if purchased Glonass license file is installed.

### Summary of Glonass support

| Receiver           | Glonass available?             | Requirements                                                                                                                                                                          |
|--------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| uBlox M8T          | Yes                            | A) v5.7.0 or above: just uBlox receiver (license file no longer needed)<br>B) v5.1.5 to 5.6.0 or below: multi-GNSS license required                                                   |
| Trimble RES-SMT-GG | Yes (versions 5.1.5 and above) | A) v5.7.0 or above: just Res-SMT-GG receiver (license file no longer needed)<br>B) v 5.1.5 to 5.6.0 or below: multi-gnss license<br>C) versions prior to 5.1.5: Glonass not available |
| Trimble RES-T      | No                             | N/A – Glonass Not available                                                                                                                                                           |

## C) QZSS option (reception only available if SecureSync is located in Japan/its neighbors or Australia)

**Note:** QZSS is also referred to as “MICHIBIKI”

**email from Josh (19 Jun KW)** MICHIBIKI is simply the nickname given to the QZSS system that is referred to in our manual. So the answer to your question about MICHIBIKI is yes. MICHIBIKI also supported officially.

- QZSS capability was added in software update version 5.3.0 (Sept 2015)
- (Versions 5.6.0 and below) QZSS capability requires the Glonass license file to purchased/installed (QZSS is included with Glonass)
- QZSS option not available with Trimble Res-T receiver or with software versions 5.2.1 and below.
- QZSS is only displayed if the Glonass/QZSS license file is installed (license file not required in v5.7.0 and above)

**Email from Josh (15 Sept 15)** The QZSS constellation moves in a figure of 8 , the top half covers Japan as well as her neighboring countries while the bottom half covers Australia.

The last I checked a couple of months ago, the folks Down Under are not considering QZSS as yet but that is not to say that they will not in the future.

## Summary of QZSS support

| Receiver           | QZSS available?                | Requirements                                                                                                                                                                                     |
|--------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| uBlox M8T          | Yes                            | <p>A) v5.7.0 or above: just uBlox receiver (license file no longer needed)</p> <p>B) v5.3.0 to 5.6.0 or below: multi-gnss license</p>                                                            |
| Trimble Res-SMT-GG | Yes (versions 5.3.0 and above) | <p>A) v5.7.0 or above: just Res-SMT-GG receiver (license file no longer needed)</p> <p>B) v5.3.0 to 5.6.0 or below: multi-GNS license</p> <p>C) versions prior to v5.3.0: QZSS not available</p> |
| Trimble Res-T      | No                             | N/A – QZSS Not available                                                                                                                                                                         |

### Enable or Disable Beidou/Glonass/QZSS/GPS

- Version 5.7.0 adds all constellations to be available for selection
- (versions 5.6.0 and below only) “SS-Opt-GNS” license file needs to be installed

**Note:** update version 5.7.0 (Jun 2017) alleviates the need to purchase the multi-GNSS license if its desired to add additional constellations beyond just GPS. Once a unit has been updated to 5.7.0 or above, the unit has the ability to enable GPS and other satellite constellations (units with just GPS before updating will just have GPS enabled after updating. But they can then go in and enable other constellations if desired.

**GPS/Glonass/Beidou/QZSS** (if these license files are installed, in 5.6.0 and below) are enabled/disabled in the [Interfaces](#) -> [GNSS Reference](#) page of the browser. Then click on the “Gear” box between “GNSS 0” and the indication of how many satellites are being tracked (below the photo)

**Note:** if neither GPS nor Glonass is enabled, it defaults to **GPS** being active.

#### A) Via CLI interface (telnet/ssh)

Also you could try this command from the CLI; This will enable GPS, Glonass and Galileo.

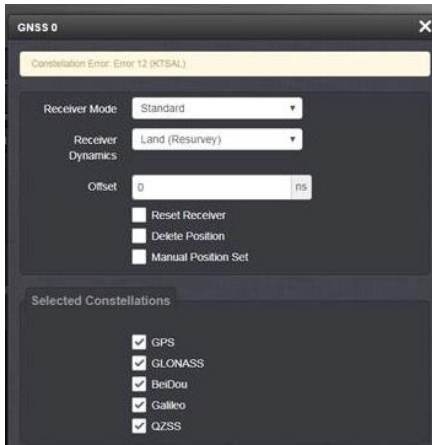
**GR\_SetConstSel 0 0 11**

This will enable just GPS and GLONASS.

**GR\_SetConstSel 0 0 10**

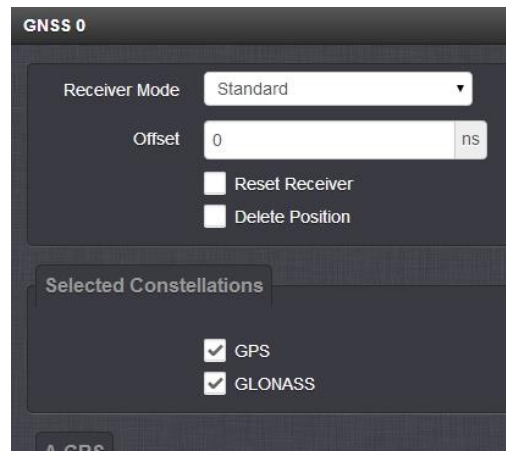
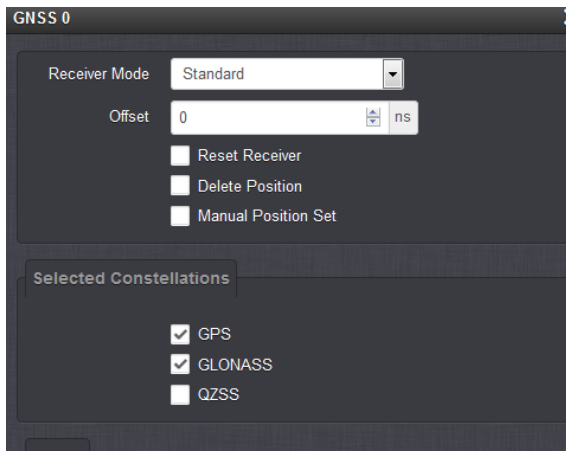
#### B) Via web browser

(Versions 5.7.0 and above?- GPS, Glonass, Beidou, Galileo and QZSS)



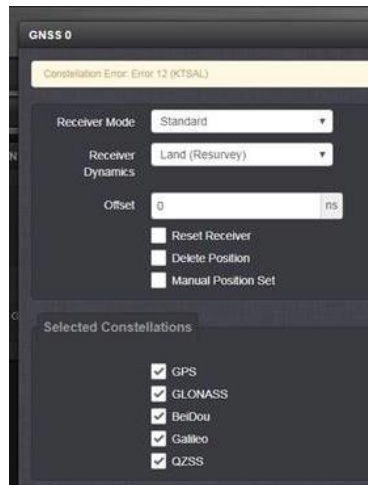
(Versions 5.3.0 and above- GPS, Glonass and QZSS)

(Versions 5.2.1 and below- GPS and Glonass)



**Valid Constellation combinations/Error message displayed: “Constellation Error: Error 12 (KTSAL)”**

- Refer to SecureSync online user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/GNSS\\_Constell.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/GNSS_Constell.htm)



Error message displayed at top of window: **“Constellation Error: Error 12 (KTSAL)”**

Q I had an error message when I select BEIDOU.

**A per Dave L 24 Jan 2018:** The GNSS receiver cannot be configured to use all the available constellations simultaneously. Here is a chart from the User Manual showing which combinations are valid.

Multi-GNSS reception: Yes, within these permissible settings:

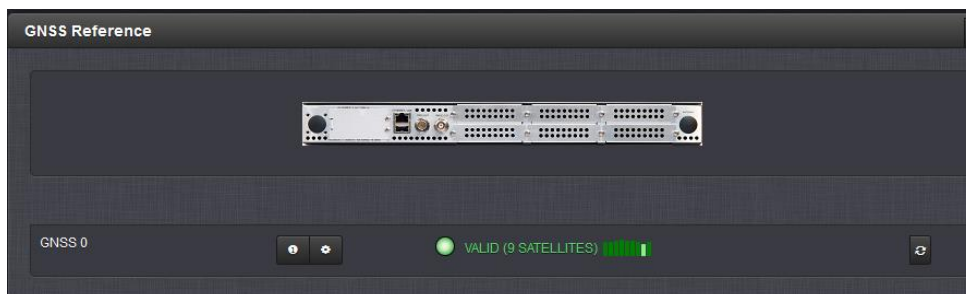
| GPS | Galileo | GLONASS | Beidou |
|-----|---------|---------|--------|
| X   | X       | -       | -      |
| X   | X       | X       | -      |
| X   | X       | -       | X      |
| X   | -       | X       | -      |
| X   | -       | -       | X      |
| -   | X       | X       | -      |
| -   | X       | -       | X      |
| -   | -       | X       | X      |



**Note:** The augmentation systems SBAS and QZSS can be enabled only if GPS operation is configured.

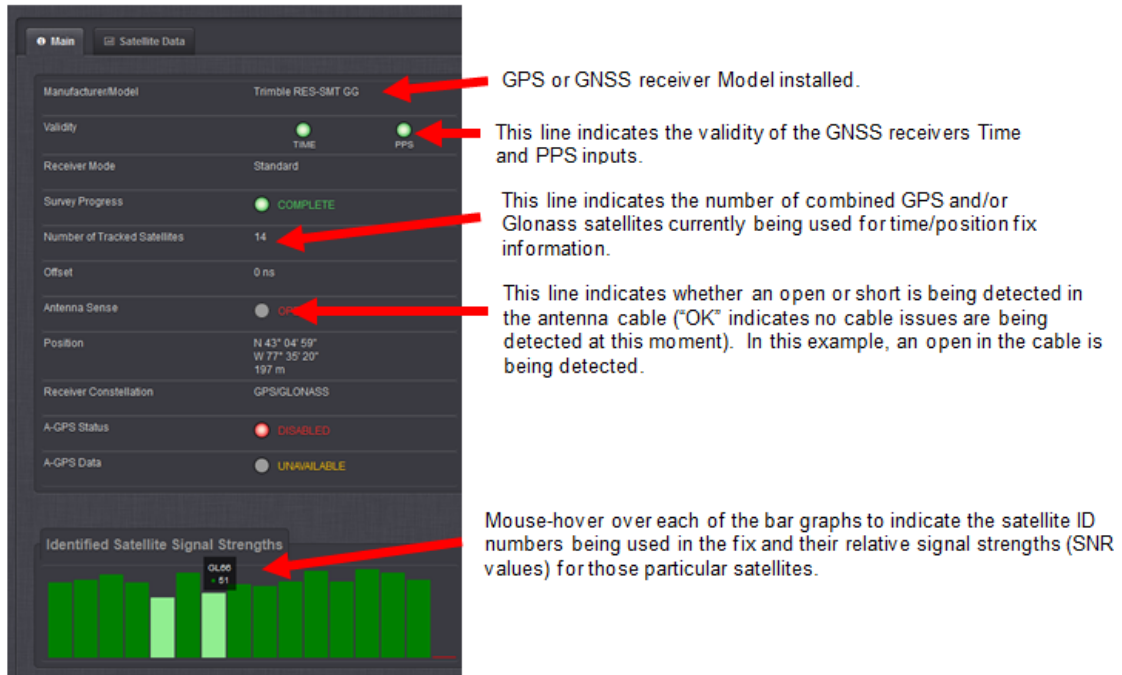
## Number of tracked GPS/Glonass/Galileo/Beidou/QZSS satellites

To determine the number of satellites currently being tracked, log in to the SecureSync's Web UI. The **Interfaces -> GNSS** page of the browser reports the number of satellites being tracked.



## GNSS Signal Status view

For a detailed view, from this page, click on the “circled i” ICON in the bottom row, under the photo. Or from the main menu, click on “**Interfaces**” at the top of the page and in the drop-down, select “**GNSS 0**”. The “**Main**” tab should be automatically selected (as shown below):



### GNSS Signal Status view (Trimble Res-T or Res-SMT-GG)

- **Red bars:** (really bad) less than??
- **Yellow bars:** SNR values of less than 35?
- **Light green bars:** SNR values from 35 to 39??
- **Darker green bars:** SNR values of 40 or greater?

The “**GNSS 0 Input Status**” page will indicate the current number of GPS and/or Glonass satellites being used in the positional fix (based on the number of vertical bars being displayed). If this field indicates no bars, it is currently not tracking any satellites. If this field indicates a low number of bars, such as only “1”, “2” or “3”, the unit is tracking a few satellites, but it’s not tracking the minimum number of satellites required for initial sync.

**(ID field) Distinguishing between GPS satellites and Glonass satellites, when the Glonass/QZSS Option is enabled**

- [http://manuals.spectracom.com/SS/Content/Global/Topics/GNSS/View\\_GNSS\\_Ref\\_Status.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/GNSS/View_GNSS_Ref_Status.htm)



| Letter Symbol | GNSS Constellation |
|---------------|--------------------|
| G             | GPS                |
| R             | GLONASS            |
| E             | Galileo            |
| J             | QZSS               |
| C             | BeiDou             |
| I             | IRNSS              |

- To determine if each bar represents a GPS or a Glonass satellite, Mouse-hover each bar to see a report of three values (two letters, the Satellite ID number and the signal strength value for that satellite).
  - **GPS** satellites are indicated with “**G**” (v5.3.0 and above) or the two letters of “**GP**” (v5.2.1 and below)
  - and have a Satellite ID Number of 0 to 59.

**Additional constellations besides GPS only available if the SS Opt-GNS License is installed (v5.6.0 and below only)**

- **Glomass** (Russia) satellites are indicated with an “**R**” (v5.3.0 and above) or the two letters of “**GP**” (v5.2.1 and below) the two letters of “**GL**” and have a Satellite ID Number of 60 and above.
- **Galileo** (Europe) satellites are indicated with an “**E**”
- **QZSS** (Japan) satellite(s) are indicated with a “**J**”. Note these satellites are only available in software versions v5.3.0 and above and if the Glonass option is enabled.

**Note:** QZSS is also referred to as “**MICHIBIKI**”

**email from Josh (19 Jun KW)** MICHIBIKI is simply the nickname given to the QZSS system that is referred to in our manual. So the answer to your question about MICHIBIKI is yes. MICHIBIKI also supported officially.

- **BeiDou:** satellite(s) are indicated with a “**C**” Note these satellites are only available in software versions 5.4.0 or above, with a u-blox Model M8T receiver installed and Opt-GNS license enabled (Started shipping this receiver ~17 March 2016 with approximate Serial Numbers 11718 and above).
- **IRNSS** (India): satellite(s) are indicated with a “**I**”.

## \*\*GR\_GetSatData 0 0 CLI command (undocumented command)

### Breakdown of the Satellite Data table:

**ch:** Receiver channel Number

**id:** (SVN) Space Vehicle Number/ID Number of the satellite being tracked

**st:** signal strength of the satellite being tracked

**t:** TRAIM (aka "**bTrain**") Is satellite accepted by the TRAIM algorithm? ("0" if no, "1" if yes)

**f:** fix status (aka "**bInfix**") Is satellite being used in the fix? ("0" if not in fix, "1" if satellite is being used in fix)

**fl:** flags reported by the receiver (always "00" with Res-T, RES-SMT and RES-SMT-GG receivers. Used only with SAASM receivers)

```
spadmin@Spectracom ~ $ GR_GetSatData 0 0

GR (0) Sat Data:
##:  ch  id  st  t  f  fl
-----
00:  00  G01  48  0  1  700
01:  01  G10  52  0  1  700
02:  02  G11  47  0  1  700
03:  03  G12  55  0  1  700
04:  04  G14  52  0  1  700
05:  05  G18  41  0  1  700
06:  06  G22  43  0  1  700
07:  07  G24  42  0  1  700
08:  08  G25  56  0  1  700
09:  09  G31  49  0  1  700
10:  10  G32  52  0  1  700
11:  11  E01  39  0  1  700
12:  12  E04  41  0  1  700
13:  13  E07  45  0  1  700
14:  14  E11  42  0  1  700
15:  15  E12  40  0  1  700
16:  16  E19  44  0  1  700
17:  17  E20  40  0  0  700
18:  18  E30  41  0  1  700
19:  00  U00  00  0  0  000
20:  00  U00  00  0  0  000
21:  00  U00  00  0  0  000
22:  00  U00  00  0  0  000
23:  00  U00  00  0  0  000
24:  00  U00  00  0  0  000
25:  00  U00  00  0  0  000
26:  00  U00  00  0  0  000
27:  00  U00  00  0  0  000
28:  00  U00  00  0  0  000
29:  00  U00  00  0  0  000
30:  00  U00  00  0  0  000
31:  00  U00  00  0  0  000

spadmin@Spectracom ~ $
```

## \*\*\*GNSS Satellites/Signal Strengths (Signal to Noise) graphs

### 1. Newer (black/charcoal browser)

- Refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/Global/Topics/GNSS/View\\_GNSS\\_Ref\\_Status.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/GNSS/View_GNSS_Ref_Status.htm) (excerpted below):

- **Identified Satellite Signal Strengths:** Bar graphs for all satellites detected. Color indicates signal strength. With your mouse pointer, hover over a bar graph to display tool tip information about satellite constellation, satellite number, and signal strength.

| Letter Symbol | GNSS Constellation |
|---------------|--------------------|
| G             | GPS                |
| R             | GLONASS            |
| E             | Galileo            |
| J             | QZSS               |
| C             | BeiDou             |
| I             | IRNSS              |

- GPS graphs not available in classic interface web browser (new browser in version 5.1.0 and above only)
- Graphs are in the newer black/charcoal browser only (software versions 5.1.2 and above only)
- Graphs are displayed in the *Interfaces* -> *GNSS 0* page of the browser, **Main** and **Satellite Data** tabs
- Hover over graphs to see specific values at a particular moment (a small dot will show in the top line to indicate a specific point where the mouse hover is reading the data from).
- Graphs show up to one week of data.
- GPS graph data is stored in the mysql database, or the SQLite database starting in v5.3.1 (not in the "log" directory). Refer to info below on exporting this data as either a **.csv** or **.json** file.
- If Satellite Data graphs aren't displayed (as shown below), switch back to the "Main" tab and then switch back to the "Satellite Data" tab again to refresh this

### 1. Main tab (bar graph at the bottom)

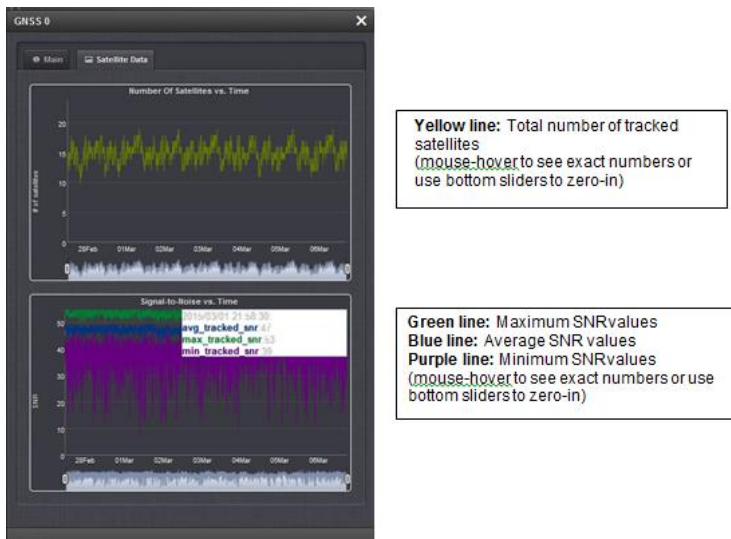
The screenshot shows the 'Main' tab of the GNSS receiver interface. It displays the following information:

- Manufacturer/Model:** Trimble RES-SMT GG
- Validity:** TIME and PPS (both green indicators)
- Receiver Mode:** Standard
- Survey Progress:** COMPLETE (green indicator)
- Number of Tracked Satellites:** 14
- Offset:** 0 ns
- Antenna Sense:** OFF (grey indicator)
- Position:** N 43° 04' 59" W 77° 35' 20" 197 m
- Receiver Constellation:** GPS/GLONASS
- A-GPS Status:** DISABLED (red indicator)
- A-GPS Data:** UNAVAILABLE (grey indicator)
- Identified Satellite Signal Strengths:** A bar graph showing signal strength for multiple satellites. One bar is highlighted with a tooltip showing 'GL06' and '51'.

Red arrows point to the following elements with explanatory text:

- Manufacturer/Model: GPS or GNSS receiver Model installed.
- Validity: This line indicates the validity of the GNSS receivers Time and PPS inputs.
- Number of Tracked Satellites: This line indicates the number of combined GPS and/or Glonass satellites currently being used for time/position fix information.
- Antenna Sense: This line indicates whether an open or short is being detected in the antenna cable ("OK" indicates no cable issues are being detected at this moment). In this example, an open in the cable is being detected.
- Identified Satellite Signal Strengths: Mouse-hover over each of the bar graphs to indicate the satellite ID numbers being used in the fix and their relative signal strengths (SNR values) for those particular satellites.

## 2. Status tab (line graphs for # of Sats tracked, and SNR)



## 3. Classic interface browser

Status -> Inputs -> onboard references

| GPS INPUT STATUS             |                    |
|------------------------------|--------------------|
| Manufacturer/Model           | u-blox M8T         |
| TPPS Validity                | Not Valid          |
| Time Validity                | Not Valid          |
| Receiver Mode                | Standard           |
| GPS Longitude                | 877° 31' 26.000" W |
| GPS Latitude                 | 847° 04' 58.200" N |
| GPS Altitude                 | 100.029 m          |
| Survey Prog                  | 99%                |
| Number of Tracked Satellites | 0                  |
| Offset                       | 0 msec             |
| Antenna Status               | Open               |

### Issue with Min SNR/Max SNR values being displayed backwards (v5.7.1 and below)

- Applies to v5.7.1 and below (expected to be corrected in update v5.7.3, ~ Feb/March 2018)

### Issue with graphs potentially not always being displayed in the browser

With at least 5.3.0 and below, graph data may not always be displayed after switching from **Main** to **Satellite** tab. Switch back to Main and then switch back to the Satellite tab again to see the data. This is a very minor issue with the refreshing that should occur when selecting the other tab.

### Storage, Exporting and Clearing of the raw satellite data used to generate the graphs

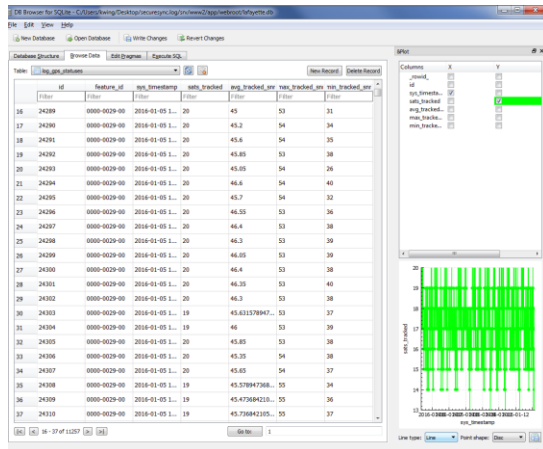
- The raw data for the generation of the graphs is stored in the MySQL database (versions 5.3.0 and below) or in the SQLite database which is exported as part of the savelogs bundle (versions 5.3.1 and above)
- Versions 5.3.1 and above download the satellite data as part of the save and download logs bundle (**Management** -> **Log Configuration** page), Data is included with the SQLite data placed in the /srv folder
- The raw data for the generation of the graphs can be exported (via browser or CLI) as either a “.csv” (can open in Excel) or “.json” file (for graphing) using the web browser

## Summary of downloading/exporting Satellite data

There are two main ways to download the satellite data for graphing. One method allows a freeware program to both display and graph the raw data after downloading a saved log bundle from the time server. The other method allows the raw data to just be downloaded as either a .csv or .json file.

Note the method to display and graph the data with a freeware program requires software version 5.3.1 (the latest available version) be installed in the time server. Downloading the raw data as either a .csv or .json file just requires the use of the new (black/charcoal) web browser which was implemented in version 5.1.2.

### 1. View the raw data and graph in the freeware “Sqlite DB browser” program (requires software versions 5.3.1 or above be installed in the time server)



**Pre-requisite:** Download/install the freeware program “dB browser for SQLite”: <http://sqlitebrowser.org>

- If the current software version is 5.3.0 or below, upgrade the software to versions 5.3.1 or above to change the MySQL database to SQLite database.
- With software versions 5.3.1 or above installed, “Save and download logs” (**Management -> Log Configuration** page of the browser)
- Use the Sqlite DB Browser program to view the database (database file is named “lafayette” and is located in the `/srv/www2/app/webroot` directory of the saved log file. Rename this file as “lafayette.db”)
- In the DB browser, open the database and then select the “**Browse Data**” tab. In the “Table” drop-down, select “**log\_gps\_statuses**” in the Plot table, select desired fields to be graphed.
- Data can be saved (as .png, .jpg, PDF or .bmp file) by pressing to “Save” ICON in the upper-right corner.

### 2. Output the raw satellite data as either a .csv or json file (versions 5.1.2 and above – including 5.3.1 and above)

Output of raw satellite data as a “csv” file (can be opened in excel)

Note: This method works with MYSQL Database (versions 5.3.0 and below) or with SQLite (versions 5.3.1 and above)

**Email from Ron Dries (18 Nov 15)** If you manually enter `/Logs/gpsStatusLog.csv` after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

**Example:** <http://10.10.128.1/Logs/gpsStatusLog.csv> (change address as applicable) (link is cap-letter sensitive)

I have tried this in Chrome and it worked. I haven't tried it in any other browser.

**Example file download below**

|    | Date/time       | # tracked        | Avg | Max         | Min (SNRs) |
|----|-----------------|------------------|-----|-------------|------------|
| 1  | 1 0000-0029-00  | 11/18/2015 21:45 | 9   | 45.22222222 | 51 40      |
| 2  | 2 0000-0029-00  | 11/18/2015 21:46 | 10  | 43.7        | 51 34      |
| 3  | 3 0000-0029-00  | 11/18/2015 21:47 | 10  | 44.3        | 51 40      |
| 4  | 4 0000-0029-00  | 11/18/2015 21:48 | 10  | 44          | 51 38      |
| 5  | 5 0000-0029-00  | 11/18/2015 21:49 | 9   | 44.77777778 | 51 40      |
| 6  | 6 0000-0029-00  | 11/18/2015 21:50 | 10  | 44.2        | 51 39      |
| 7  | 7 0000-0029-00  | 11/18/2015 21:51 | 10  | 44.6        | 51 41      |
| 8  | 8 0000-0029-00  | 11/18/2015 21:52 | 7   | 45.42857143 | 52 42      |
| 9  | 9 0000-0029-00  | 11/18/2015 21:53 | 7   | 45.71428571 | 52 43      |
| 10 | 10 0000-0029-00 | 11/18/2015 21:56 | 7   | 44.85714286 | 52 39      |
| 11 | 11 0000-0029-00 | 11/18/2015 21:57 | 7   | 44.57142857 | 52 37      |
| 12 | 12 0000-0029-00 | 11/18/2015 22:00 | 7   | 43.71428571 | 52 37      |
| 13 | 13 0000-0029-00 | 11/18/2015 22:01 | 7   | 44.42857143 | 52 38      |
| 14 | 14 0000-0029-00 | 11/18/2015 22:02 | 7   | 44.14285714 | 51 36      |
| 15 | 15 0000-0029-00 | 11/18/2015 22:03 | 8   | 43.635      | 51 36      |

### Automating the generation of the .csv file (being provided via CLI interface)

- Dave Sohn created a python script file that automates a .csv file being generated via CLI interface. Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\GPS\python script for gps info](#)

### Output of graphable data (as a “.json” file for graphing)

**Note:** This method works with MYSQL Database (versions 5.3.0 and below) or with SQLite (versions 5.3.1 and above)

- Same process as downloading.csv file, but replace “.csv” with “.json” instead.

If you manually enter `/Logs/gpsStatusLog.json` after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: <http://10.10.128.1/Logs/gpsStatusLog.json> (change address as applicable) (link is cap-letter sensitive)

### Example file download below

```

10.10.128.1/Logs/gpsStatusLog.json
[{"id": "24274", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "45.578947368421", "max_tracked_snr": "52", "min_tracked_snr": "40"},
{"id": "24275", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "46.105263157895", "max_tracked_snr": "52", "min_tracked_snr": "39"},
{"id": "24276", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "46.210526315789", "max_tracked_snr": "52", "min_tracked_snr": "39"},
{"id": "24277", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "46.263157894737", "max_tracked_snr": "51", "min_tracked_snr": "39"},
{"id": "24278", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "46.157894736842", "max_tracked_snr": "51", "min_tracked_snr": "38"},
{"id": "24279", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "46.157894736842", "max_tracked_snr": "51", "min_tracked_snr": "38"},
{"id": "24280", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "46.368421052632", "max_tracked_snr": "51", "min_tracked_snr": "38"},
{"id": "24281", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "19", "avg_tracked_snr": "46.368421052632", "max_tracked_snr": "51", "min_tracked_snr": "38"},
{"id": "24282", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "20", "avg_tracked_snr": "46.05", "max_tracked_snr": "50", "min_tracked_snr": "40"},
{"id": "24283", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "20", "avg_tracked_snr": "45.25", "max_tracked_snr": "50", "min_tracked_snr": "37"},
{"id": "24284", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "20", "avg_tracked_snr": "45.15", "max_tracked_snr": "50", "min_tracked_snr": "37"},
{"id": "24285", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "20", "avg_tracked_snr": "45.15", "max_tracked_snr": "50", "min_tracked_snr": "37"},
{"id": "24286", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "20", "avg_tracked_snr": "45.15", "max_tracked_snr": "53", "min_tracked_snr": "36"},
{"id": "24287", "feature_id": "0000-0029-00", "sys_timestamp": "2016-01-05",
  "data_tracked": "20", "avg_tracked_snr": "45.15", "max_tracked_snr": "53", "min_tracked_snr": "36"}

```

### Alignment of 1PPS output from receiver to system, based on the Satellite constellation selected (not applicable to Trimble Res-T GPS receiver)

- Refer to Mantis case 2938 for details
- **Summary:** SecureSync 1PPS output can be offset (by up to 300ns) depending on which GNSS constellations are selected. Different timescales have different definitions of their 1PPS Signal.

### \*\*GPS Reception/receiver troubleshooting/issues with GPS reception

- Refer to: [GPS\GPS reception Ap Notes\SecureSync](#)

## Bent center plate on rear panel Type N GPS input connector

- Search for “**Bent center plate**” in the Custserviceassistance document

Note: this condition of one of the four plates being spread out too far has resulted in at least one instance where the GPS RF signal was still getting in (receiver was tracking satellites) but the antenna problem alarm was still asserted.

### Email Keith sent to a customer (2 Aug 16) regarding an RMA with internal coax cable replaced due to a bent plate- receiver still tracking satellites but Antenna Problem alarm was asserted

The picture below from the cable that was replaced shows exactly what the condition was and allows me to be able to easily explain what inadvertently happened to this connector after it was shipped from the factory.

The center of this rear panel connector that makes contact with the center pin of the building cable is formed by four small plates. The tech found that one of these plates had been pushed apart from the other three plates, affecting the shape of the center connection (the plate to the upper-left in the picture below):



When the building cable is attached to the back of the time server on this threaded connector, if this cable connector starts off as being cross-threaded (before being backed-off and reconnected), the center pin of the cable can go into these plates at an angle, causing one or more of the plates to be pushed apart from the others.

This picture above was a very peculiar incident in where there was just enough contact with the center pin that the GPS signal was still able to reach the GNSS receiver (it was still able to track satellites). But the 5vdc that is outputted from the receiver to power the antenna had less current draw than expected. The receiver was sensing this as an open in the antenna cable and therefore was asserting the Antenna Problem alarm (this alarm indicates the receiver is detecting either an open or short in the antenna cable). Normally if the receiver is able to track satellites, the 5vdc is fine son the antenna problem alarm wouldn't be asserted.

I have seen this condition with a bent plate happen before, where the cross-threaded connector has pushed the plates apart. But it usually causes a complete loss of RF and the antenna problem alarm to be asserted. This is the first I've seen where the plate being bent out still allowed RF to get through to the receiver, but also caused an issue with the 5vdc current draw.

---

## \*\*GPS Antenna Problem alarm

### Antenna Sense = “unknown”

It sounds like the internal GPS receiver may have suffered a power surge or lightning strike. The “unknown” state is indicating that the GPS receiver's antenna sense circuit (which measure the current draw of the 5vdc used to power the GPS antenna) is detecting some type of problem with the GPS antenna connection, but can't tell what the problem is. This is an abnormal indication for the GPS receiver to be reporting. It would not be caused by any normal failure of either the antenna connection or with the GPS antenna itself. If the GPS receiver suffered a surge, the antenna may or may not have also been affected.

**For troubleshooting this condition-** treat it as if there is an open or short in the antenna cable.

- **GPS preamp or splitter installed-** these devices can block the detection of an open/short in the cable on the antenna side of the device (the device draws current, so the receiver thinks there is a good connection to the antenna, even though the antenna is not getting any voltage.

### One or more of the four center plates of the rear panel GPS input connector may be spread out too far

**Note:** this condition of one of the four plates being spread out too far has resulted in at least one instance where the GPS RF signal was still getting in (receiver was tracking satellites) but the antenna problem alarm was still asserted.

Refer to “**Bent center plate...**”section further above and also in the Customerserviceassistance doc.

---

## Desire to clear Antenna Problem alarm when GPS antenna is not connected

**Note:** Archive Version 4.8.7 (Sept 2012) is adding the ability to disable the Antenna Problem alarm indications via the **Setup-> Notifications** page of the browser. Log entries for cable issues will still be asserted, if the alarm is disabled.

As a matter of fact, there certainly is a way to prevent the Fault LED from blinking. This is an indication that the Antenna Problem alarm is asserted, because the GPS sense circuit is detecting an open in the GPS port.

To clear this alarm, you just need to simulate a GPS antenna being connected. The output voltage of the rear panel antenna jack (used to power the antenna) is a nominal +5vdc. To simulate a GPS antenna being connected to this jack, simply put a 60 to 200 ohm resistor from the center of the antenna jack to the outer-t threaded portion of the same jack. This resistive load will simulate a GPS antenna being connected, therefore clearing the Antenna Problem alarm (the LED will no longer blink).

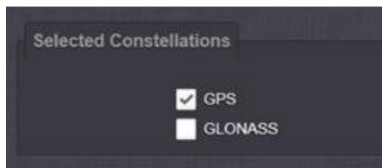
The specific resistor value doesn't really need to be a specific value. The sense circuit is pretty wide open in order to support GPS antennas with varying impedance values. We have used antennas with 67 ohm impedance as well as around 200 ohm impedance. Any value in this general range will simulate the GPS antenna being connected.

## GNSS receiver and its version stop being reported in manifest log

- Observed in 5.8.4 with ublox receiver installed

## Sporadic losses of GPS reception (one or a couple of seconds) with Res-SMT-GG receiver and Glonass being enabled (requires Glonass License be installed) (noticed ~ June 2015)

- Res-SMT-GG receiver can drop to 0 satellites for one or just a couple of seconds and then go back to great reception again (more predominant when Glonass license is installed and Glonass is enabled).
- Likely due to receiver firmware versions 1.0.7 (1.7) or 1.0.6 (1.6) being installed in the Res-SMT-GG receiver. Receiver should be updated to version 1.08 (1.8). Refer to known issues with the Res-SMT-GG receiver
- Version 1.0.8 (1.8) update is included in the version 5.3.0 release - Sept 2015). Temp work-around: Either disable Glonass or return receiver to the factory for update to firmware version 1.08 update.
- Glonass can be disabled in the **Interfaces** -> **GNSS 0** page of the newer browser (as shown below):





---

## Mobile (Continuous) mode and Single Satellite mode

### \*\*Operational Speed and Altitude limitations

#### \*\*Speed and Altitude limitations when using a commercial GPS receiver

As far as speed (and altitude) limitations for the Res-T receiver (these are common limitations across all commercial GPS receivers due to export controls).

- **Altitude** 18,000 m
- **Velocity** 515 m/s

**Note:** Either limit may be exceeded, but not both!

### GPS Receiver update rate /refresh rate

Q. What is the update rate of the GPS position information, assuming access through the CLI on SNMP?

A. The receiver updates position at a 1 Hz rate.

### Ground speed/track angle

Q Is there any way to access the ground speed or track angle information through either the CLI or SNMP?

A **Reply from Dave Lora (SR 6575)** The Front Panel, command line interface “gpsloc” command and the SNMP MIB variables for Latitude, Longitude and Altitude can be read. We do NOT recommend walking the MIB to read the data, however, reading these values at no faster than 1Hz is possible.

```
[spadmin@Barrett_SideB ~]$ gpsloc
Position:
Lat N 43 4 59.120
Lon W 77 35 20.522
Alt 168 m
```

Q Would the unit moving at moderate speeds (25 knots / 39 mph / 46kph) have any effect on the timing accuracy? If the user places the SecureSync in Mobile mode it can be used in mobile operation. The use of timing receivers in low speed, low dynamic (meaning slow turns) motion will be the lowest risk in degrading Time/1PPS signal performance depending on GNSS/GPS Receiver type installed.

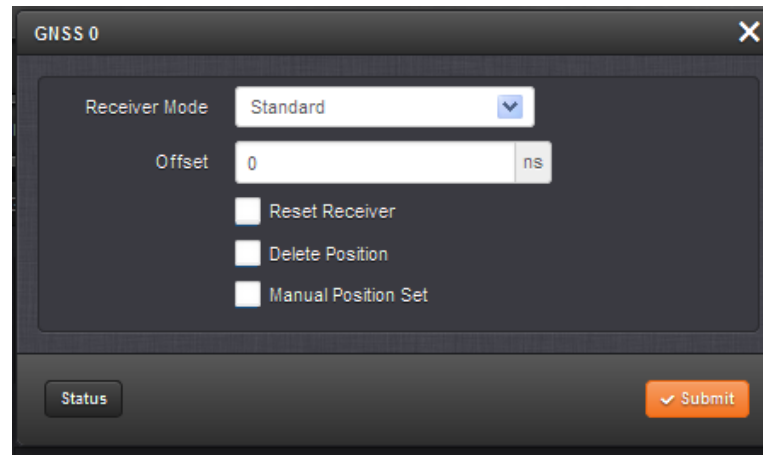
A **Reply from Dave Lora (SR 6575)** The Trimble receivers will experience degraded 1PPS performance 3x worse than our stated specification in the best case. The recommended receiver type to use is the U-Blox M8T which should suffer little to no performance loss under these conditions. It is recommended the customer use Release 5.4.1 firmware until Release 5.4.5 is available. Release 5.4.5 will display Land/Sea/Air Dynamics selection for Mobile Mode users.

### Degradation of timing/positional accuracies while in mobile mode (Continuous mode)

- The amount of degradation varies depending on whether the SecureSync has the earlier Model Res-T GPS receiver installed or a newer Res-SMT-GG GNSS receiver installed.
- Refer to either the “Trimble Res-T” or “Trimble Res-SMT-GG” receiver section in the Customerserviceassistance document for details.

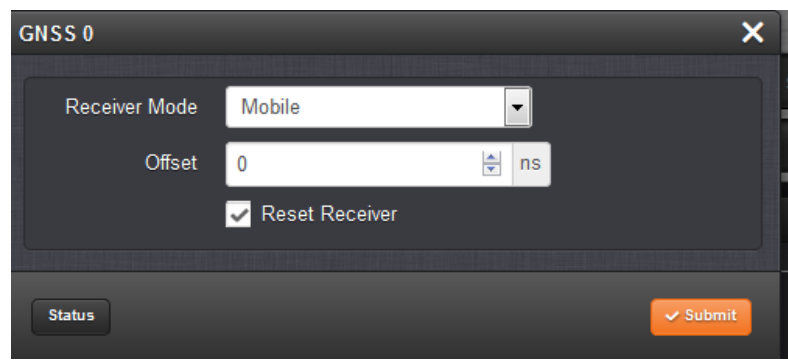
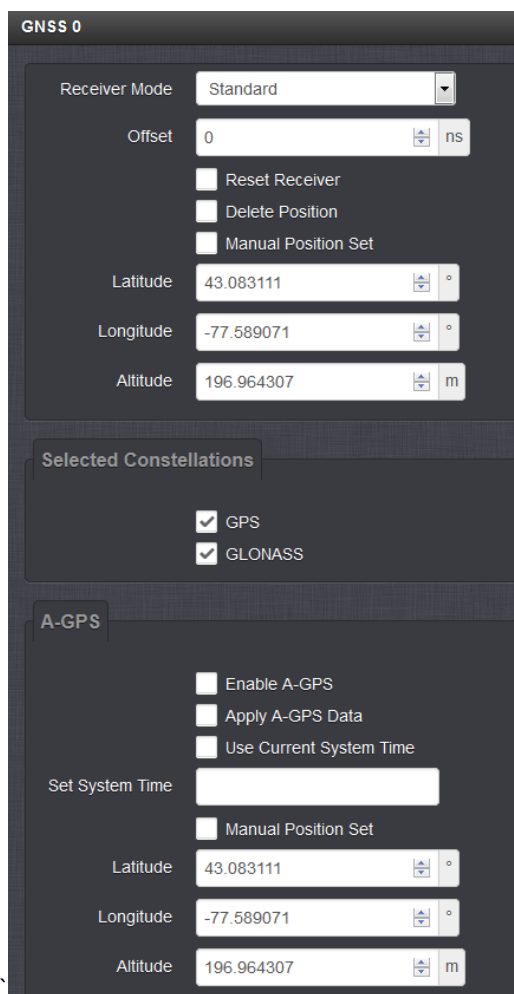
### Change the GNSS Receiver Mode (Standard, Mobile or Single Satellite) in Archive versions 5.1.2 and above)

- 1) Go to **Interfaces** -> **GNSS 0**
- 2) Click the “gear” near “**GNSS 0**”



Interfaces -> GNSS 0, Edit (Glonass Option enabled)

Interfaces -> GNSS 0, Edit (Glonass Option not enabled)



### Desire to manually set the position

- 1) Disconnect the GPS antenna
- 2) Delete the position (select **"Delete Position"** and Submit)
- 3) Select **"Manual Position Set"** checkbox

- 4) Must enter latitude, longitude and an altitude value for the manual position to be accepted.

GNSS 0

Receiver Mode: Mobile

Offset: 0 ns

Reset Receiver

Delete Position

Manual Position Set

Latitude: 43.083119 °

Longitude: -77.589032 °

Altitude: 172.473164 m

#### To manually enter the latitude

- As “**N**”: don’t add any sign at the beginning (N is +).
- As “**S**”: add a minus (-) sign at the beginning (S is -).
- Example entry for “North 43 12 34 56: 43.123456

#### To manually enter the longitude

- As “**E**”: don’t add any sign at the beginning (E is +).
- As “**W**”: add a minus (-) sign at the beginning (S is -).

Example entry for “West 077 12 34 56: **-077.123456**

#### Notes about manually setting the position via CLI interface

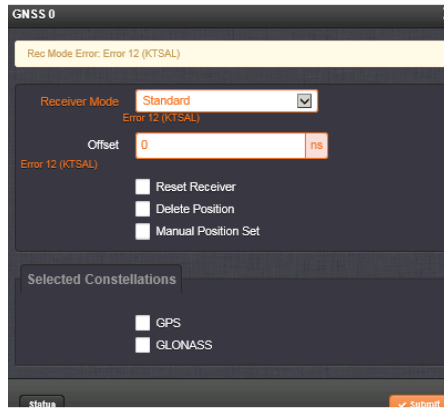
1. The KTS call for setting position is **GR\_SetPosition 0 0**, but the admin and user accounts don’t have permission to use this call to manually set the position. However, these accounts do have permission to get/display the current position using the **GR\_GetPosition 0 0** call.

```
spadmin@Spectracom ~ $ GR_GetPosition 0 0
GR (0) Position:
  Lat (deg): 43.083153
  Lon (deg): -77.589100
  Alt (m)   : 163.270096
spadmin@Spectracom ~ $
```

---

#### “Rec Mode Error: Error 12 (KTSAL)

- Refer to SR4597 in SAP (see screenshot further below)
- Reported by Wells Fargo in two SecureSyncs with v5.2.0 software installed
- They reported the GNSS receiver changed on its own from Standard to Single Satellite mode.
- They have Glonass Option enabled.
- They weren’t making any changes to the GNSS receiver configs when this condition was observed.
- Fixed with reboot.



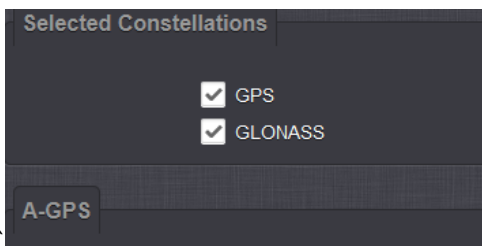
**“Constellation Error: Error 12 (KTSAL)”**: Error message displayed and “[webui] ERROR (7) - ERROR in KTSAL\_Set:

GR\_SetConstSel 0 0 0 (KTSAL)” in the System log when changing GNSS receiver configuration **“Note about Offset field**: Error 12 is also associated with changing the antenna cable offset value and pressing Submit, for the same reasons mentioned below. As discussed below, this is just an error message issue in 5.1.7 and below with RES-SMT-GG receiver installed. The offset value is still accepted though the message is displayed.

This error message is a known minor software issue (in at least versions 5.1.7 and below) associated with changing the receiver configuration with a Res-SMT-GG receiver installed and the Glonass option not enabled. Should be fixed in the Jan 2015 V5.2.0 update.

- Refer to Mantis case 2900
- Applicable to versions 5.1.7 and below, with a RES-SMT-GG receiver, and Glonass Option not enabled
- This error message doesn’t adversely affect the system in any way.
- Can occur when a user is changing GNSS receiver configuration (**Interfaces -> GNSS 0** page, Edit button)

**For internal FYI info only**: When the Glonass option isn’t enabled and a Res-SMT-GG receiver is installed in software versions 5.1.7 and below, the GPS and/or Glonass selection (shown in the screenshot below) isn’t displayed on the web page- So neither constellation can be selected by a user. The “default setting” results in an “invalid” combination, so this error message is displayed. But the user config changes that were being made when the error was displayed are still applied, even though this condition occurred. So it’s just an error message display issue.



The Fix for this issue is planned for the release sometime near the beginning of 201

**Front panel indicates receiver is tracking >4 satellites, but *Status -> Inputs -> GPS* page reports tracking only 1 satellite.**

- The **Status -> Inputs -> GPS** page of the browser will report its tracking only “1” satellite when the GPS receiver is configured for **Single Satellite mode**.

- The SNR table on this same page of the browser and the front panel (when configured to display satellites being tracked) will report the number of sats actually being tracked.
- Refer to the section below for more info on the receiver modes.

---

## “Receiver modes” (Stationary, mobile and single satellite modes)

### A) Standard Receiver mode (factory default) and GPS Survey

- With a few earlier versions of software, the GPS receiver required four satellites at all times, even after GPS survey has been completed. The minimum requirement with most newer versions of software drops to requiring just one satellite after the GPS survey has been completed (just like the Model 9200 and 9300 series).

#### GPS Survey (stationary/Standard mode only)

- GPS Survey takes 2000 seconds (33.5 minutes) to complete, once GPS receiver is tracking at least four satellites.
- GPS survey is not performed while the GPS receiver is in mobile mode.
- GPS survey only performed first time in new location, while in stationary mode. If the equipment is relocated, the survey is performed again, at the new location.
- While the GPS receiver is in stationary mode, the Status-> Inputs -> on board reference GPS page will first boot-up showing:

**Mode:** Standard (Stationary)

**Dynamics Code:** Land

- The “Survey Prog” field (Status-> Inputs -> on board reference GPS page) displays percent complete.
- Once the GPS Survey has been successfully completed, the Dynamics code changes to: “**Stationary**” and the **Survey Prog**” field changes to “**Complete**”.

---

### B) GPS Mobile mode

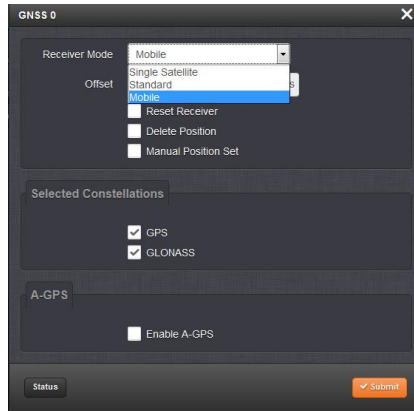
- Also **Refer to** Mobile mode operation with a Resolution-T receiver (NetClock and SecureSync)
- Mobile mode requires four satellites at all times to maintain full sync status (to prevent going into Holdover mode)

#### Receiver dynamics codes

Receiver dynamics codes for mobile mode (such as land, sea, etc.) were removed in software **version 5.0.0**.

#### 1. Versions 5.1.2 and above (newer interface)

- Mobile mode is enabled/disabled in the Interfaces -> GNSS 0 page of the browser. Then click on the “Edit” box. Select Mobile and then Submit:



- Once in mobile mode, the minimum requirement to maintain sync is for the GPS receiver to track at least four satellites at all times. Dropping below 4 will put unit into Holdover mode.
- PDOP/TDOP info- If PDOP or TDOP exceed a certain level, a log entry is added to the GPS Qualification log. High PDOP/TDOP results in less accuracy of the receiver. The lower the values, the better the timing. The rough estimate for timing accuracy is 1 meter of position error = 3.3 ns of timing error. A PDOP above 12 will stop the GPS survey from continuing if it was in a survey.
- Accuracy of the receiver while in mobile mode (and the GPS receiver is not in motion) is no better than 3 times worse than while in stationary mode. While in motion, accuracy may get even worse, depending on the PDOP/TDOP value which may be affected by the movement, such as aircraft banking.

## 2. Versions 5.0.2 and below (Classic interface)

1. Go to the **Setup -> Inputs -> on board reference GPS** page to enable mobile mode (select land, sea or air as applicable). Enabling this mode turns off the GPS survey and changes the mode to “auto-fix”.
2. Change “Receiver Mode” to “Mobile”.
3. Select the desired “Dynamics Mode” (Land, Sea or Air) (software versions 4.8.9 and below only)
4. Press Submit.

Once in mobile mode, the minimum requirement to maintain sync is for the GPS receiver to track at least four satellites at all times. Dropping below 4 will put unit into Holdover mode.

PDOP/TDOP info- If PDOP or TDOP exceed a certain level, a log entry is added to the GPS Qualification log. High PDOP/TDOP results in less accuracy of the receiver. The lower the values, the better the timing. The rough estimate for timing accuracy is 1 meter of position error = 3.3 ns of timing error. A PDOP above 12 will stop the GPS survey from continuing if it was in a survey.

Accuracy of the receiver while in mobile mode (and the GPS receiver is not in motion) is no better than 3 times worse than while in stationary mode. While in motion, accuracy may get even worse, depending on the PDOP/TDOP value which may be affected by the movement, such as aircraft banking.

---

## Single Satellite mode:

- Requires at least one QUALIFIED satellite and valid position information (either by completing a GPS survey or manually entering the correct position)
  - (versions 5.0.2 and below) The Status -> Inputs -> GPS page of the browser will report its tracking only "1" satellite when the GPS receiver is configured for Single Satellite mode.
  - The SNR table on this same page of the browser and the front panel (when configured to display satellites being tracked) will report the number of sats actually being tracked.
- 

## Desire ability to remotely disable GPS as an input reference

- The GPS input reference can be remotely disabled, if desired, without needing to physically disconnect the GPS antenna.
- Remotely change the "State" field for GPS to "Disabled"
- Once GPS "State" has been disabled, SecureSync will sync to the next highest priority reference (if one is present/valid) or it will immediately go into Holdover mode.
- The GPS receiver continues to track GPS satellites when "State" field is disabled.
- Switch the GPS "State" field back to "Enabled" to re-enable GPS input. GPS will become valid immediately and will be selected (if it's the highest priority reference).

## GPS can be remotely disabled via:

### A) Web browser

In the **Setup -> Reference Priority** table, change the **State** field for **GPS 0 / GPS 0** to "**Disabled**".

### B) CLI interface (telnet or ssh)

Use the "**stateset**" command to remotely change the **State** field of any input of the Reference Priority.

### C) SNMP

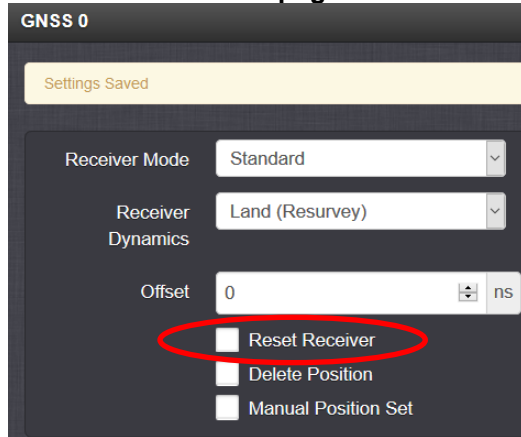
Refer to "**ssReferenceMgmtObjs**" in the **SPECTRACOM-SECURE-SYNC-MIB.mib** file for the items used to configure the Reference Priority table (specifically, see "**ssRefMgmtState**", which is used to enable or disable input references).

## Receiver reset/reset GNSS receiver

- Refer to online SecureSync user guide:  
[http://manuals.spectracom.com/SS/Content/\\_Global/Topics/GNSS/GNSS\\_recReset.htm](http://manuals.spectracom.com/SS/Content/_Global/Topics/GNSS/GNSS_recReset.htm)

The Reset Receiver command causes the GNSS receiver to execute a cold start: All data will be erased from the volatile receiver memory. Only non-volatile memory is preserved.

*Interfaces* -> *GNSS 0* page



GNSS 0

Settings Saved

Receiver Mode: Standard

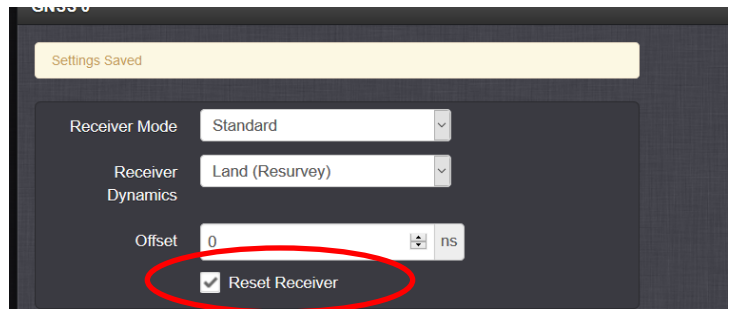
Receiver Dynamics: Land (Resurvey)

Offset: 0 ns

Reset Receiver

Delete Position

Manual Position Set



GNSS 0

Settings Saved

Receiver Mode: Standard

Receiver Dynamics: Land (Resurvey)

Offset: 0 ns

Reset Receiver

**Note:** “Delete Position” and “Manual Position Set” checkboxes disappear right after selecting the “Reset Receiver” checkbox (before pressing Submit)

## Journal log entry asserted after resetting receiver

“Set Reset for GPS Reference 0 in slot 0 to GR (0) Reset: Cold (0)”

|                    |         |                                                                   |
|--------------------|---------|-------------------------------------------------------------------|
| Oct 08<br>21:04:24 | [webui] | Set Reset for GPS Reference 0 in slot 0 to GR (0) Reset: Cold (0) |
|--------------------|---------|-------------------------------------------------------------------|



---

## User-defined Minimum Satellites alarms/traps

### A) Newer browser (Versions 5.1.2 and above)

1. User defined alarms are configured in the **Management -> Notifications** page (bottom of the **GPS** tab)

The screenshot displays a configuration interface for user-defined alarms. It is divided into two main sections: 'Minor Alarm Threshold' and 'Major Alarm Threshold'. Each section contains two input fields: 'Minimum Satellites' and 'Duration Below Threshold (s)'. The fields are currently empty, indicating they are ready for user input.

- User defined alarm can be Masked, if desired, in the **Management -> Notifications** page, **GPS** tab

### B) Classic interface browser (Versions 5.0.2 and below)

- User defined alarms are configured in the **Tools -> Notifications** page, **Threshold** tab
- User defined alarm can be Masked, if desired, in the **Tools -> Notifications** page, **GPS** tab

## Known issues associated with the user-defined alarms

### A) Tracking 1 satellite for 130 seconds with a Res-T receiver on new week rollover

- Refer to the Res-T section of the Customerserviceassistance doc for details
- New week rollover on Saturday, UTC midnight can cause the user-defined alarm to be asserted, if the Threshold is set to less than 130 seconds..

### B) Threshold counter not counting consecutive seconds (versions 4.8.8 and below)

1. (Archive versions 4.8.8 and below) Threshold counter (shared between both the Minor and Major User-defined alarms) is counting cumulative seconds below the min number of sats, instead of counting the consecutive number of seconds below the min
  - Refer to Mantis case 1956.
2. Results in User-defined alarms being asserted even when the consecutive number of seconds below the threshold field has not been exceeded. When the cumulative count below min has reached the threshold, the alarm is asserted. The Qual log may show tracking 3 sats for 3 seconds, but a User-defined alarm with a timeout of 60 seconds is still asserted
3. Likely to be observed when user-defined alarms are configured and GPS reception is often falling below the min number of satellites, going above the min, and then back below the min again.
  - This issue was addressed in the March 2013 version 4.8.9 release.

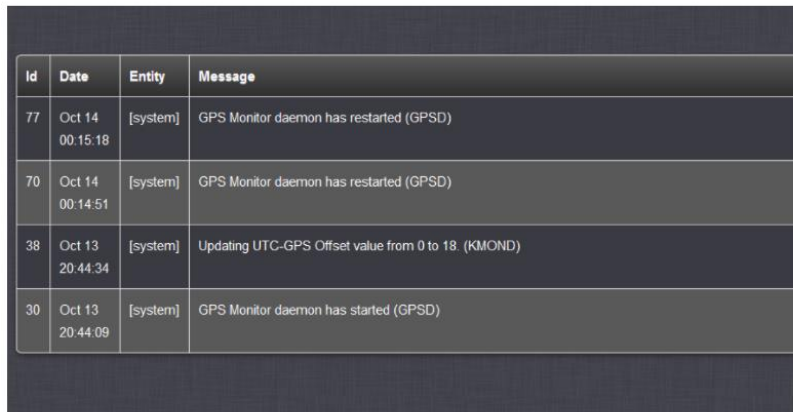
## GPSD (GPS service daemon)

- Unlike 2400 SecureSyncs/VersaSyncs, Model 1200 SecureSyncs (any software version) do not have the gpsd service program installed.
- For more info on GPSD, refer to "GPSD" in: <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>

### Reference to "gpsd" in the Model 1200 logs

- Refer to Salesforce Case 247067.

Thanks for the information. I did notice in the system log it referenced GPSD, but when I login to the shell I see gpsmond running...



| Id | Date            | Entity   | Message                                             |
|----|-----------------|----------|-----------------------------------------------------|
| 77 | Oct 14 00:15:18 | [system] | GPS Monitor daemon has restarted (GPSD)             |
| 70 | Oct 14 00:14:51 | [system] | GPS Monitor daemon has restarted (GPSD)             |
| 38 | Oct 13 20:44:34 | [system] | Updating UTC-GPS Offset value from 0 to 18. (KMOND) |
| 30 | Oct 13 20:44:09 | [system] | GPS Monitor daemon has started (GPSD)               |

```
spadmin@phx1-r7r10-ntp-01 ~ $ ps -ef | grep gps
root      2712    1  0 Oct13 ?        00:07:06  gpsmond
spadmin  10261  12456  0 17:59 pts/2    00:00:00  grep --colour=auto gps
spadmin@phx1-r7r10-ntp-01 ~ $
```

Is the log in the UI referencing the gpsmond but outputting GPSD?

**Keith's response (20 Oct 2021)** A very astute observation!! I had to look at the screenshot to see exactly what you were referring to. You are the first to mention this!

The "GPSD" in these logs entries is not referring to the "GPSD" package which "collects data from a Global Positioning System receiver and provides the data via an Internet Protocol network to potentially multiple client applications in a server-client application architecture" (and has the date issue about to occur this weekend). The Model 1200 SecureSyncs do not have this software package installed.

The "GPSD" and "GPSMOND" being referred to in the log entries are associated with the SecureSync-specific software that interfaces with its GNSS receiver to output the GNSS receiver data to the rest of its software (such as via the web browser or SNMP). Unlike the Model 2400 SecureSyncs, which do have the gpsd software package installed, the 1200 SecureSync do not have a direct serial interface to its GNSS receiver (which is what the GPSD service program provides).  
**interface to its GNSS receiver (which is what the GPSD service program provides).**

---

## SAASM GPS receivers (Rockwell Collins GB-Gram /Trimble Force-22)

Available SAASM receivers:

### A) Model 1204-1A (Rockwell Collins GB-Gram Model MPE-S receiver)

- Refer also to the SS Option Card document for more details: <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>
  
- Rockwell Collins P/N for the GB-Gram MPE-S receiver : 987-9705-X01

### Min GPS signal level at input

**Email from Paul Myers:** "Dennis H at Rockwell Collins said he would recommend no more than 8dB loss between Antenna and MPE-S receiver."

---

### B) Model 1204-07 (Trimble Force 22e receiver)

- Refer also to the SS Option Card document for more details: <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>

### Battery disconnect switch

- Like the Model 1204-1A Option Card, the 1204-07 also has a battery disconnect switch
- (~9 Dec 16) Per Dave West, apparently two SecureSyncs were recently shipped with a metal plate that does not have a hole in the metal to be able to access the shut-off switch.

---

## SAASM GPS Receiver operation

- Links to documents about SAASM:

(2/3/12) **Important Note:** do not email information on SAASM, because our servers are hosted in Europe.

### A) For 9300 series

- **\*\*\*Unreleased 9300 SAASM addendum:** <U:\Engineering\SAASM-FOUO\CustomerService> (not released – do not distribute).

#### Other reference documents

- [I:\Company Wide\Project Folders\Rainier\(938x\)\400 Customer Service Plan\Tech Notes](I:\Company Wide\Project Folders\Rainier(938x)\400 Customer Service Plan\Tech Notes)
- The <U:\Engineering\SAASM-FOUO\Docs & Tools\Crypto Key Ordering> folder contains a document for ordering crypto
- The <U:\Engineering\SAASM-FOUO\Docs & Tools\Crypto Key Ordering> folder also contains a document for the Model 9300 SAASM operation

### B) For SecureSyncs

- SecureSync SAASM receiver Manual Addendum (1200-5000-0053) Note: NOT in Arena as it's a FOUO document: <U:\Documentation\Released\Manuals\1200-xxxx-xxxx>
- (SecureSync only) The <U:\Engineering\SAASM-FOUO\Released\Manuals> folder contains the Spectracom doc regarding SAASM keyloading (loading keys, key status, and warning messages)

---

## Dept of Defense Form DD-1494 (DD1494 for SAASM)

- Refer to: ["I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8225S\DD-1494 Form"](I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8225S\DD-1494 Form)

**Email from Dave L to Morgan Randolph** This must be an extended version of the DD-1494. There is a section Receiver Equipment Characteristics form on page 3 dealing with the receiver and Antenna Equipment Characteristics on page 4 form for the 8225S antenna . That is what the customer was asking about. Can we provide this information to them?

**Reply from Morgan Randolph to Dave L (12 May 2020)** Hey Dave, this should be what you need: <https://www.rolia.com/documents/8225s-datasheet>

Hiro says we do not need a DD-1494 for the VersaSync because it is not transmitting.

Hi Morgan,

The Versasync does not emit any RF so a DD-1494 is not required. It's only required if you have an emitter (transmitter). (See the section labeled " APPLICATION PURPOSE" in the instructions page.)

-Hiro

---

## Troubleshooting a SAASM GPS reception issue

If the GPS receiver has been keyed and is having any difficulty tracking satellites (not tracking any satellites or is tracking a low number of satellites)

- 1) Zeroize the receiver.

- 2) See if it starts tracking a normal number of satellites (>4)
- 3) Re-key the receiver after at least an hour.
- 4) Verify it continues to track while being keyed.

---

## **Known potential issue with GB-Gram (MPE-S) SAASM receiver going into Holdover for 1 second**

### **A) MPE-S sometimes enters holdover at 12:01-12:02 UTC**

- Refer to MANTIS Case 2641

### **SAASM GPS Option Cards**

- **GB-GRAM** (GBGRAM/GB Gram): SAASM GPS receiver (stands for Ground-Based GPS Receiver Application Module). Designed as a low cost SAASM GPS receiver for ground-based (ARMY) applications.

---

### **Type of SAASM Receiver installed**

- **To determine type of SAASM receiver installed, refer to:** <U:\Engineering\SAASM-FOUO\CustomerService\SAASM Receivers>

### **GB-Gram SAASM receiver installed**

- Two types of GB-GRAM receivers (Type 1 and Type II)
- Refer to: <U:\Engineering\SAASM-FOUO\CustomerService\SAASM Receivers\GB-Gram receivers>

---

### **Replacement SAASM components**

1. **Front panel Keyfill connector / zeroize switch wiring harness (wiring, connector and switch): CA08R-MT00-0001**
  - Refer to PD: 1200-0017-0600 for picture of this assembly.

---

### **SAASM Key operation**

- **link to documents about SAASM:** <U:\Engineering\SAASM-FOUO>

### **CONTACT:** Rolf Speziale

Zeli Systems  
33 Pagosa Ct  
El Paso TX 79904  
(915) 751-3222  
[gps@zeli.com](mailto:gps@zeli.com)  
KLIF account is ZELI001 (ID of the SAASM Facility)

---

### **Simple Key Loader (SKL)**

- **Refer to:** [U:\Engineering\SAASM-FOUO\CustomerService\SKL \(Simple Key loader\)](U:\Engineering\SAASM-FOUO\CustomerService\SKL (Simple Key loader))

---

## Standard Positioning Service (SPS) mode

This is the unkeyed mode of SAASM receiver operation. To verify operation in SPS mode:

1. Simply attach the antenna and verify the NetClock is in Sync.
2. Look at the GPS Signal Status page for L1 Only satellites. (SPS)
3. See Security SAASM page and verify unkeyed.

---

## Key Storage

- Refer customers to Rockwell Collins

Q (from Salesforce Case 190594) Also, do you have any documentation that verifies this component stores key material to support up to 30 days of operation without key fill?

A (Reply from Ron Dries 22 April 2019) For the keys question, Spectracom/Orolia is unable to answer that question. The customer will need to speak with Rockwell Collins.

---

## Number of Keys remaining

- Refer to: <U:\Engineering\SAASM-FOUO\CustomerService\Key expiration>
- 

## Low battery power indicator

### Email from Paul Myers

In preparation for the update to the SAASM addendum, here is what a low battery SAASM GPS condition looks like.

You will see this message in the Operational Log.

Mar 13 17:04:06 Spectracom spectracom: [system] GPS Warning (11): Low memory battery

Mar 13 17:09:06 Spectracom spectracom: [system] GPS Warning (11): Low memory battery

The Force 22E (and MPE-S GB-GRAM) will post a similar message in the SecureSync Timing log.

---

## Desire to convert a commercial GPS input to a SAASM GPS receiver

Email from Dave Sohn on 11/17/11 (for a customer of Florise with Les Ullis):

There is a lot involved with converting a unit from standard Res-T to SAASM, and that is before the controlled item issues.

1. The physical assembly steps are involved to convert from Res-T to SAASM
2. The front panel needs to be changed and the key fill / zeroize cable needs to be attached. This involves first removing the AC/DC converter and front panel PCB.
3. The battery holder and battery needs to be installed.
4. The Res-T and antenna cable needs to be removed.
5. The SAASM option card and SAASM unit need to be installed and cabled, including the new antenna cable.
6. The serial number label needs to be replaced showing the new model and serial number with the required SAASM prefix.
7. The unit also needs to be updated with the new model number and a patch to tell the SW about the removal of the Res-T.
8. We would not be able to test functionality of the option card, SAASM, and cabling together, which is a risk.

Dave Lorah also mentioned the Factory password would need to be provided in order to make the necessary configuration changes in the web browser.

---

## Troubleshooting/known issues with SAASM receivers

- Refer also to <U:\Engineering\SAASM-FOUO\CustomerService>

**Note: Always capture the receiver firmware and hardware version info (via a screenshot of the interface (INTERFACES > REFERENCES > SAASM GPS 0 page of the browser, “Versions FOUO” tab)**

**In at least version 5.8.2 and below, not all this info is captured in the Manifest log z**

### Known issues/conditions with Gb-Gram receivers

**Note: Always capture the receiver firmware and hardware version info (via a screenshot of the interface (INTERFACES > REFERENCES > SAASM GPS 0 page of the browser, “Versions FOUO” tab)**

- In at least version 5.8.2 and below, not all this info is captured in the Manifest log
- **Refer to “known issues” doc in:** [U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A \(GB-GRAM\)](U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A (GB-GRAM)) )

#### 1. GPS Antenna Sense circuit doesn't operate correctly (as observed in 5.7.1)

- Refer to Salesforce case 127507
- Refer to “known issues” doc in: [U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A \(GB-GRAM\)](U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A (GB-GRAM))

#### 2. Issue with SAASM key errors, if keyed SecureSync (GB GRAM receiver only) runs undisturbed (not power cycled/rebooted) continuously for more than around 49- 53 days

- May see “**GPS Warning (51): RAIM exclusion failed**” in logs (as observed in Salesforce Case 179497)
- Refer to SF cases such 133596 (Aug, 2016 as reported by Ken Parks) 215424/215423 (for Navair)
- For all details of this issue (including fix), refer to the “Known issues with GB GRAM SAASM receivers” document in the US Only drive ( [U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A \(GB-GRAM\)](U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A (GB-GRAM)) )
- **Important Note (per Paul Myers 28 Nov, 2017)** do not mention or discuss this issue, or the fix, with any customers without first talking with either Paul or Dave Sohn first!

#### 3. SecureSyncs with GB-GRAM receiver can potentially go into Holdover mode for 1 second.

- Refer to Mantis case 2641
- Refer to “known issues” doc in: [U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A \(GB-GRAM\)](U:\Engineering\SAASM-FOUO\CustomerService\SecureSync\1204-1A (GB-GRAM)) )

**Summary:** SOMETIMES MPE-S SAASM GPS SecureSyncs will enter holdover for 1 second when reading the UTC-GPS offset and testing for pending Leap Second Adjustments.

---

## M-Code (M Code) receiver/capabilities

- Forward to OGS!

Q Question from Keith: Hi Dave (Tony, Mike, Wade and Steve),

Just got a call from Jerome ? with NGC inquiring if SAASM SecureSyncs are currently M-Code compliant.

Wasn't really sure what we could say on this topic (such as for future plans). Told him not currently and gave him Tony's number for additional info on this topic. For tech support, what general type of info/future plans/timeframes, etc can we provide on this?

**A Reply from Tony Diflorio (10 Jan 17)** My story to our customers (and I am sticking to it☺) is that we have it in our roadmap to add M-Code capability to our SecureSync when the M-Code receivers are available to integrators such as Spectracom. At this time, M-Code production receivers are not available. David can correct me if I am wrong...

---

## SBAS

- As of at least version 5.7.1 (Oct, 2017), SBAS is NOT supported in SecureSync/9400s
- I have not heard of any intentions for SBAS support to be added.

---

## Obtaining/Loading SAASM keys

- Refer to "SecureSync SAASM manual addendum" (1200-0000-0053): <U:\Engineering\SAASM-FOUO\CustomerService\SecureSync>

**Note:** Upload to customer using ARMDEC website: <https://safe.amrdec.army.mil/safe/> (Select "non CAC users").

An automatic email will be sent to you to verify the sender. The requested password to use for the verification will be included towards the bottom of this auto-email (example: "The Password is: Q\$#2975!99?62J\*2\*3!J")

---

## Opt-SEM (Option SAASM Modulation)/ Time Mark Data Message (ID 3)

- See Paul Myers or Scott Hildebrandt for details
- Applicable to SAASM receiver units only .
- Was initially a special for a customer (3DLLR/ Raytheon C-Band Radar project)
- Per Paul Myers "OPT-SEM provides ICD-GPS-153C messaging on the 1204-02 ASCII Output for the Time Mark Data Message (ID 3) Allows the SecureSync to emulate the message coming directly from the installed SAASM receiver
- Verify with Scott Hildebrandt
- Provides data from the ICD-GPS-153 interface, specifically the Time Mark Data Message (ID 3).
  - Time Mark Data Message is apparently an on-time marker from a SAASM receiver.

**Per Paul Myers (23 Jan 17)** Opt-SEM was validated on the MPE-S Type II GB-GRAM, but should work for Force 22E.



---

## T1 and E1 input

**Note (16 Jun 2016):** T1 (DS1) and E1 input are **NOT** currently available as input references (There are currently no T1 or E1 input Option Cards available. All T1/E1 Option Cards are currently output only cards).

According to Dave Sohn, there are no plans at this time to incorporate T1/E1 inputs.

---

## \*\*MSF/WWVB/DCF77

### Email from Dave Sohn (7/24/12)

There are no plans for radio time signals like MSF, WWVB, and DCF77 in the SecureSync/NetClock 9400 products at this time. Our alternatives for GPS signal failure are to provide holdover during the failure period with our OCXO and Rubidium oscillator options, if they do not have supported alternative time signal sources available.

---

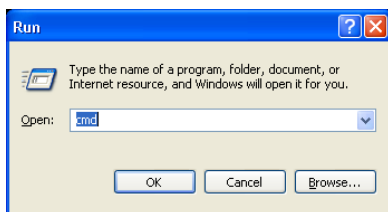
## SecureSync thinks a GPS receiver is installed but really isn't (such as a SecureSync 011)

A "Remove GPS Patch" (SSO4-1200) is FTP'd into the SecureSync during Manufacturing to mask the GPS functionality. If the unit reports GPS alarms (such as Antenna Problem alarm) with no GPS receiver installed, this software patch must have been inadvertently not installed. The patch file can be installed remotely if FTP port is open, by logging into FTP using the spfactory account password (do not provide this password to ANUY customers)!

The patch file is located at: [I:\New Released\Firmware\\_Software\1200-xxxx-xxxx\1200-SS04-1000](I:\New Released\Firmware_Software\1200-xxxx-xxxx\1200-SS04-1000).

The instructions to apply this patch (from the SecureSync factory test procedure) are listed below (This procedure is explaining how to FTP transfer the patch into SecureSync).

1. Copy F/W from controlled drive to local C:\TEMP.
2. From Start Menu on PC, select Run and type cmd <ENTER>.



**CAUTION:** All patch files have same name. Ensure correct file is selected for installation or UUT will not function properly for customer. In some cases, the wrong file will not display any errors until sufficient data has been logged.

```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>c:
C:\>cd temp
C:\Temp>ftp 192.168.1.63
Connected to 192.168.1.63.
220----- Welcome to Pure-FTPd [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 17:39. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server
220 You will be disconnected after 15 minutes of
User (192.168.1.63:(none)): spfactory
331 User spfactory OK. Password required
Password:
230 User spfactory has group access to: spuser spadmin spfactor root
230 OK. Current directory is /home/spfactory
ftp> bin
200 TYPE is now 8 bit binary
ftp> cd /tmp
250 OK. Current directory is /tmp
ftp> put patch_img.bin
200 PORT command successful
150 Connecting to port 1244
226 File successfully transferred
226 0.002 seconds (mean) 0.000 bytes per second
ftp: 1024 bytes sent in 0.002 seconds (512.000Kbytes/sec.)
ftp> quit
221 Goodbye. You uploaded 1 and downloaded 0 kbfiles.
221 Logout.

C:\Temp>

```

```

c:\ Telnet 192.168.1.57
Linux 2.6.15-USAGI (Spectracom) (0)
Spectracom login: spfactory
Password:
[spfactory@Spectracom ~]$ cd /tmp
[spfactory@Spectracom tmp]$ ls
diskversion patch_img.bin
[spfactory@Spectracom tmp]$ TSyncUpgrade 0

Starting EEPROM upgrade process.

Image file:
Mark: 0xDEADBEEF
Type: 0x00000006
Length: 0x0000002A
Version: 1.00
CRC: 0xD73F7C6C

Sending... done

Upgrade status: 100% complete...

```

3. Repeat Step 12 for any additional patch installs needed.
4. Reboot UUT by typing “**reboot;exit**” and allow UUT to reboot.
5. Using PROCOMM, select metakey **FACTORY** and **PASSWORD**.
6. Type **HALT** to power down UUT and disconnect all connections.

---

## GPS receiver FAQs

Q Does the SecureSync support manual entry of location/coordinates and altitude? (manual appears to indicate this is the case) If so, what format(s) can the coordinates be entered in (lat/lon, MGRS, etc.)?

A Yes. Info is entered as lat/lon/alt in degrees,minutes,seconds and meters.

---

Q We are considering use of the RS-232 NMEA output module. Assuming it outputs data reflective of the source currently used by the SecureSync. For example, if manual coordinates were entered rather than using GPS coordinates automatically, would the NMEA sentences include the manually entered coordinates in lieu of what would normally come from GPS?

A NMEA outputs are reflective of the current system information including position. Assuming the position information was set manually and accepted by the GPS reference/receiver, they would be used for the NMEA data. Refer to the SecureSync manual for the specific NMEA message formats provided.

---

## \*\*T1/E1 and AFNOR input time references

- refer to: [..\SecureSync Option Card information.pdf](#)

---

## \*\*External 1PPS input (epp0)

- There is no 1PPS input on the base SecureSync (Option Card is required)
  - Refer to [..\SecureSync Option Card information.pdf](#)
- In summary: External 1PPS input requires the use of one or more installed 1PPS input Option cards, such as the following (Refer to: Specific Option Cards)
  - **Model 1204-01:** Single ended input
  - **Model 1204-02:** Balanced differential input
  - **Model 1204-28:** TTL single ended input
  - **Model 1204-1D:** non-isolated 1PPS input on a BNC connector
  - **Model 1204-2A:** Fiber Optic (1) 1PPS in and (2) 1PPS outputs
  - **Model 1204-2B:** Fiber Option (4) 1PPS outputs

**1PPS Input impedance: 50 ohms**

**NTP/External 1PPS input requires a unique change to ntp.conf file via NTP Expert mode**

- refer to refer to (in this doc): [NTP/External PPS input](#)

### **NTP/ External 1PPS input references**

**Important Notice:** Using NTP and external PPS input as the selected references requires **NTP Expert mode be enabled** so the ntp.conf file can be manually edited. Failure to edit the ntp.conf file in Expert mode degrades the performance of the SecureSyncs outputs (including PTP) and the system does not take advantage of the external PPS accuracies.

For more info, refer to (in this doc): [NTP/External PPS input](#)

---

## **“Frequency 0” (Freq 0) external input frequency (such as 10 MHz input)**

- Refer to [..\SecureSync Option Card information.pdf](#)
- Frequencies of 1kHz to 10 MHz can be inputted into SecureSync via Option Cards
- Refer to Models 1204-01 and 1204-03 Option Cards in the SecureSync Option Card document
  - 1204-01: TTL in (single-ended input)
  - 1204-03: RS-485 n (Balanced input)

With Frequency input cards (such as 1204-01 or 1204-03), a 1 kHz to 10 MHz (sine or square wave) frequency can be inputted in order for SecureSync to generate a 1PPS from this signal.

---

## \*Reference Status table

Reference Status is viewable via browser:

### A) Newer black/charcoal browser (v5.1.2 and above)

### B) Classic interface browser

- At the bottom of the *Status* -> *Time and Frequency* page of the browser.

| REFERENCE STATUS |           |           |
|------------------|-----------|-----------|
| Reference        | Time      | 1PPS      |
| GPS 0            | OK        | OK        |
| IRIG 0           | OK        | OK        |
| NTP              | OK        | OK        |
| User             | Not Valid | Not Valid |
| Local System     | OK        | OK        |

**User reference:** Only “OK” (valid) after the time is set and it only remains valid if it becomes the selected reference.

**NTP Reference:** Only “Valid” right after NTP is qualified. It will only remain “Valid” if becomes the selected reference. Otherwise goes to “Not Valid” normally displayed. ”

### Refer to Knowledge Base Article

<https://na8.salesforce.com/knowledge/publishing/articlePreview.apexp?id=kA0C00000008X5K&popup=true&pubstatus=d&preview=true>

**Note (22 Jul 13 KW) :** Per Dave Sohn, the NTP Ready LED will blink green for one second every 60 seconds, when NTP is not the selected reference, at the moment NTP input is valid.

**Note:** NTP may periodically and temporarily select an NTP server (before switching back to the System Time reference, for example). In this scenario, NTP will go momentarily valid and then back to not valid again, because NTP is no longer synced to another NTP server.

- User and NTP references only go “valid” when they become the selected reference. They do not remain valid if they aren’t selected (they remain not valid when they aren’t selected. with NTP, it’s the selected reference, when NTP selects another Time Server to be its selected reference (as displayed on the NTP-> Status page or in the NTP log).

**NTP (and User” mode) are two unique input references that are only “valid” when they are selected as the input reference. When other references are the selected refer(Email Keith sent to customer 8/8/12) ence (instead of NTP) , “NTP” (and User) will remain “not valid” in the “Reference Status” table. The other configured higher Stratum NTP servers are verified each second as being available for selection, but their validity isn’t “confirmed” until NTP needs to be selected as the input reference (either NTP is configured as the highest reference in the Reference Priority table, or all higher priority references have since been lost and NTP is the next highest available reference). Once NTP is selected, the Reference Status table will then show NTP as being valid.**

As shown in this screenshot above, NTP is currently yellow and indicating “Not Valid”. There is a reason that NTP remains yellow, instead of turning green like other references in this table do (such as GPS). Unlike many other input references, NTP (and User set time) only turn green when they are the selected input reference.

To see NTP go to “OK”, and with GPS the only other input reference applied, you can easily and temporarily disable GPS input, to allow NTP to become the selected reference. Navigate to the **Setup-> Reference Priority** page of the browser. In the row that lists “GPS 0” in both columns, temporarily change the “State” field to “Disabled” and hit “Submit”. This will disable GPS input, causing the next highest priority reference to be selected, until GPS input is enabled again. With NTP input being the next highest priority value, NTP will now be selected as the input reference. The Reference Status table should now show NTP as “OK” (in green).

Now go back to the Reference Priority table and re-enable the GPS row. Because GPS is a higher priority reference than NTP, it will automatically switch back to GPS being the selected reference. The Status table for NTP will go back to

reporting its "Not Valid", unless GPS input is lost/declared not valid again.

**PTP Reference:** "PTP 0" will indicate "**Not Valid**" for one of two reasons.

- 1) When the PTP Module is configured as a PTP Master, this entry will always indicate "Not Valid".

When the PTP module is configured as a PTP Slave, it will indicate "Not Valid" until the SecureSync has been synced to a PTP Master, which is connected to the Ethernet port of the PTP module (whether connected directly with a network cross-over cable or through network hubs and switches. Once connect to a PTP master, the PTP Module should achieve sync within about a minute of connecting the Ethernet cables.

- 2) With PTP 0 being enabled in the Input Reference Priority Table (Setup/ Reference Priority page of the web browser) and with it being the highest valid priority reference, SecureSync will declare its in sync using PTP as its selected reference.

## \*\*Time Sync / Holdover mode

### Holdover

The SecureSync user guide has a good description of Holdover mode

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/Holdover.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/Holdover.htm)

- Holdover value is stored in the ktsif.conf file
- ktsif.conf file is located in home/spectracom/config directory

### Slight Delay before going into Holdover mode, once satellite reception is lost

- Due to a past observed issue w/SAASM receivers dropping to 0 sats for like 1 second, since then there is an intentional delay of a few seconds after receiver reports tracking 0 sats before time server actually goes into Holdover mode. It no longer transitions into Holdover the moment the receiver reports tracking 0 sats.

### Typical oscillator holdover rates (from the SecureSync manual)

| Oscillator Type               | Typical Error Rates after 4 hrs | Typical Error Rates after 24 hrs |
|-------------------------------|---------------------------------|----------------------------------|
| Low Phase noise Rb (Rubidium) | 0.2 $\mu$ s (nominal)           | 1 $\mu$ s (nominal)              |
| Rb (Rubidium)                 | 0.2 $\mu$ s (nominal)           | 1 $\mu$ s (nominal)              |
| High performance OCXO         | 0.5 $\mu$ s (nominal)           | 10 $\mu$ s (nominal)             |
| Standard OCXO                 | 1 $\mu$ s (nominal)             | 25 $\mu$ s (nominal)             |
| TXCO                          | 12 $\mu$ s (nominal)            | 450 $\mu$ s (nominal)            |

Table 3-3: Estimated oscillator error rates during Holdover

### Configuring the length of Holdover Timeout

- The timeout value is configured in seconds with a valid range of 1 second up to 5 years. The default holdover period is 2 hours (7200 seconds).

#### **From the SecureSync user guide:**

Holdover Timeout is a user-configurable allowable time period in which SecureSync remains in Holdover mode before it declares loss of synchronization. Holdover Timeout can be adjusted according to personal requirements and preferences. The factory default Holdover period is 2 hours..

**Note:** Changes made to the Holdover Timeout always take effect immediately. If SecureSync is in holdover and the Holdover Timeout is changed to a value that is less than the current time period that SecureSync has been Holdover Mode, the unit will immediately transition to out of sync.

### Holdover value greater than 30 days can potentially result in Leap Second time error

Configuring a Holdover value exceeding 30 days could result in a one-second time error in the UTC or Local timescales until an external reference (GNSS or IRIG input) is restored or a manually configured Leap Second is asserted by a user (leap seconds do not affect the GPS and TAI time scales).

## Holdover timeout is configured in “seconds”

| Desired Holdover Length | Holdover Length (in seconds) to be entered |
|-------------------------|--------------------------------------------|
| 2 hours                 | 7200 seconds (default value)               |
| 24 hours                | 86400                                      |
| 7 days                  | 604,800                                    |
| 30 days                 | 2,419,200                                  |
| 1 year                  | 29,030,400                                 |
| 5 years                 | 10,450,944,010                             |

### A) Configure via the CLI

- Read current Holdover value: **SS\_GetHoldoverTo 0** <enter> (in seconds)
- Change Holdover value: **SS\_SetHoldoverTo 0 xxxx** <enter> (in seconds)

### B) Configure via the web browser

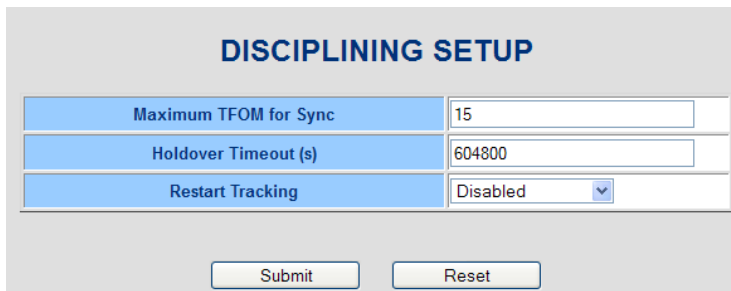
#### 1. Archive versions 5.1.2 and above

The length of Holdover is configured in the **Management -> Disciplining** page and then clicking on the “gear” next to “**Status**” (in seconds)



#### 2. Classic web browser (versions 5.0.2 and below)

The length of holdover is set in the **Setup/Disciplining** page of the web browser.



The value is configured in seconds with a valid range of 1 second up to 5 years. The default holdover period is 2 hours (7200 seconds).

When a valid input is connected, the SecureSync is in sync, and not in the holdover mode. Once the input is lost, for a certain duration, the SecureSync will go into the holdover mode of operation. During this interval



(default Holdover is 2 hours), the time is being derived from the SecureSync's oscillator and so it also remains in the sync mode in addition to the holdover mode being active. If the external reference is restored before the holdover period expires, the SecureSync remains in sync, but holdover is turned off. If two hours elapses with the reference not returning, both sync and holdover are then removed.

| Desired Holdover Length | Holdover Length (in seconds) to be entered |
|-------------------------|--------------------------------------------|
| 2 hours                 | 7200 seconds (default value)               |
| 24 hours                | 86400                                      |
| 7 days                  | 604,800                                    |
| 30 days                 | 2,419,200                                  |
| 1 year                  | 29,030,400                                 |

### Nice detailed Holdover mode draft

Excellent point about the desire to appear as “synchronized” even upon loss of either unit's input reference(s). There is a built-in mode of operation just for this reason. This available mode of automatic operation is called the Holdover mode. Holdover mode starts when all of its input references (as configured in the Reference Priority table) are lost or become not valid. Holdover mode ends when one of the following events occurs:

At least one input reference becomes present and valid again

The Holdover period times-out before at least one input reference becomes valid again

The unit power cycles (it doesn't boot back-up into Holdover mode, without first going back into Sync mode).

While it's in Holdover mode, the System Time (and therefore also NTP) is maintained by a 1PPS signal generated by the internal 10 MHz oscillator. In Holdover mode, the unit is treated as if it's still in full sync mode. The outputs are still fully useable while it's in Holdover mode.

The length of holdover is configured in the **Setup -> Disciplining** page of the web browser. The value is configured in seconds with a valid range of 1 second up to 5 years. The default holdover period is 2 hours (7200 seconds).

When a valid input is connected, the SecureSync is in sync, and not in the Holdover mode. Once all inputs are lost/ declared not valid (GPS tracking 0 satellites for instance, or the Slave no longer able to talk to the Master), the SecureSync will go into the Holdover mode of operation. During this interval (the default allotted Holdover period is 2 hours), the time is being derived from the SecureSync's internal oscillator and so it also remains in the sync mode in addition to the Holdover mode being active. If the external reference(s) is restored before the holdover period expires, the SecureSync remains in sync, but Holdover is turned off. If the Holdover period elapses with no reference(s) returning by then, both sync and Holdover modes are then removed.

The table below, from the SecureSync user manual, provides the conversion of commonly desired Holdover periods into seconds.

| Desired Holdover Length | Holdover Length (in seconds) to be entered |
|-------------------------|--------------------------------------------|
| 2 hours                 | 7200 seconds (default value)               |
| 24 hours                | 86400                                      |
| 7 days                  | 604,800                                    |
| 30 days                 | 2,419,200                                  |
| 1 year                  | 29,030,400                                 |

The better the stability of the 10 MHz oscillator type installed, the more accurately maintained the System Time will be while in the Holdover mode. For examples, the typical time drift during Holdover of a TCXO oscillator is about 5 seconds/month, for the OCXO oscillator is about 52 milliseconds/month or for the Rubidium oscillator is about 130 microseconds/month. Using these typical values, and based upon your typical time accuracy requirements, they can then be used to calculate how much of a Holdover mode period can be tolerated, before loss of sync occurs to prevent the outputs from being useable.

#### **“Time Sync” is true when:**

- The SecureSync is in full sync with one of its input references (In this state, “Holdover” is false).
- The SecureSync is in Holdover mode (all input references are lost, but the Holdover period has not yet expired). (In this state, “Holdover” is also true).

#### **Time Sync is false when:**

- 1) All input references are no longer present/valid and the Holdover mode has since expired. (In this state, “Holdover” is also false).
- 2) The unit first boots-up and has not yet synced to any input reference. (In this state, “Holdover” is also false).

#### **“Time Sync” is true when:**

- The SecureSync is in full sync with one of its input references (In this state, “Holdover” is false).
- The SecureSync is in Holdover mode (all input references are lost, but the Holdover period has not yet expired). (In this state, “Holdover” is also true).

#### **Time Sync is false when:**

- 1) All input references are no longer present/valid and the Holdover mode has since expired. (In this state, “Holdover” is also false).
- 2) The unit first boots-up and has not yet synced to any input reference. (In this state, “Holdover” is also false).

## **Holdover mode**

**Important note:** Drift is non-linear!

**Email from Dave Sohn (17 Oct 2013)** Drift in holdover is not linear as implied here. The phase drift will be exponential as the frequency drifts. So, no oscillator will provide <1ms per day indefinitely. For example, the TSync OCXO will provide less than 1ms per day for around 6-7 days, but more than that afterwards. Also, all of our models are based on good starting values starting out from GPS synchronization, which won't be available here.

**Email from Tony Diflorio to a potential customer looking for 1ms/day accuracies** A couple of other ideas to help you: You could use a portable (battery operated) GPS synchronization device to provide re-synchronization to the TSync-PCIe-Opt-OCXO card, such as our model GPS-12/12R (see attached). This re-synchronization would have to be done every few days though to maintain the TSync-PCIe-OCXO to <1ms per day of drift. Or, you might be able to use our popular “SecureSync”, rack mounted GPS Synchronization system (see attached) with a Rubidium internal oscillator. This depends on whether you must have specific features that only a Bus-Level card can provide. Using our SecureSync with a Rubidium internal oscillator will provide the holdover accuracy you are looking for, over a much longer period of time (almost indefinitely).

The holdover mode begins when all input references are considered invalid and ends when either at least one input is considered valid or until the holdover period expires.

## **Holdover FAQs**

**Q** Why is the default holdover value 2 hours

**A** As for 7200 seconds of default holdover- this equates to 2 hours of holdover, which just happened to be the same value as the "worst-case" NetClock (With TCXO oscillator installed). Because the default Holdover value is not linked to the type of on-board oscillator, Engineering went with the default of the NetClock with TCXO being 2 hours of holdover. This value is customer configurable for up to 5 years.

Q Are there any holdover performance specifications for the high-stability Rubidium internal clock option? We have a specific requirement of no more than 1 microsecond of drift per day when operating on internal clock for timing.  
A Holdover specs are provided in the datasheet. The standard Rubidium holdover spec for 1 day is 2us.

**Known potential issue with GB-Gram (MPE-S) SAASM receiver going into Holdover for 1 second**

**1. MPE-S sometimes enters holdover at 12:01-12:02 UTC**

- Refer to MANTIS Case 2641
- 

**\*\*Local interference, GPS jamming and GPS Spoofing**

- Refer to: “GPS Spoofing and GPS jamming” in the “Custserviceassistance” PDF document

---

## Oscillators/ disciplining to 1PPS input reference/TFOM/1PPS phase error

**\*\*Types of available Oscillators/installed oscillator type**

**Which type oscillator is installed?**

A) CLI command to determine type of oscillator installed: **oscget <enter>** or **XO\_GetOscType 0**

```
spadmin@Spectracom - $ oscget
OCXO (5ppb)
spadmin@Spectracom - $
```

B) Web browser report of oscillator installed

- **Newer browser:** The installed oscillator type is reported in the “**Oscillator Type**” field located in the top-left corner of the *Management* -> *Disciplining* page.
- **Classic interface web browser:** The installed oscillator type is reported in the “**Oscillator Type**” field in the *Status* -> *Time and Frequency* page.

### Types of Oscillators that can be installed

1) **Low Phase Noise Rubidium” or “Low Phase Noise Rb” (Y100R-0002-RC04) (SecureSync-x5x, such as SecureSync-051 or SecureSync-057 for examples)**

- Displayed in browser as: “**LPN Rubidium (.1ppb)**”
- Consists of the Low phase noise OCXO oscillator combined with the SpectraTime SRO-100 Rubidium oscillator  
*(9/28/12 design in progress)* Will provides the low phase noise specs of an OCXO combined with the greater stability of installed Rb oscillator. The Rb oscillator will lock to GPS and output a very stable 1PPS to discipline the OCXO oscillator.

**Our P/N for the two oscillators combined: Y100R-0002-RC04**

- “**Y100R-0002-RC04**” consists of two combined internal oscillators:

1. **SpectraTime SRO-100 Rb oscillator**

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Rb oscillator>
- Our PN: Y100R-0002-RC03 (see additional info further below)

2. **Morion MV197 low phase noise OCXO**

- see info further below for “**LPN OCXO**”
- Our P/N: Y100R-0002-PH10

---

2) **Standard Rubidium oscillator (SpectraTime SRO-100) (also the RB osc for Harris) (SecureSync- x3y, such as SecureSync-031, SecureSync-033 or SecureSync-037 for examples )**

- Displayed in browser as (I believe): “**Rbxo (.5ppb)**”
- “**Option 4**” in Models 9483 and 9489
- Uses SRO-100 Rb oscillator from SpectraTime (<\\Rocfnp01\drivedata\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Rb oscillator>)
  - **Our P/N:** Y100R-0002-RC03

**MFG:** SpectraTime

MFG. P/N and description: **SRO-100/10M/12V/NO60/F/S/E**

- **In Arena at:** [https://app.bom.com/items/detail-spec?item\\_id=1202848069&version\\_id=10268167148](https://app.bom.com/items/detail-spec?item_id=1202848069&version_id=10268167148)
- link to SRO-100 manual: [http://www.spectratime.com/documents/iSync\\_SRO-100%20SynClock%20Manual\\_140522.pdf](http://www.spectratime.com/documents/iSync_SRO-100%20SynClock%20Manual_140522.pdf)
- Link to SRO-100 data sheet: <http://www.spectratime.com/products/isync/gps-disciplined/SRO-100/>
- Also refer to: “SRO-100 Rubidium oscillators” in the Customerserviceassistance document

**L3Harris replacement oscillator advisory (2021): IPN 13 #2**

---

#### **Rubidium/Hazardous material in SRO-100 oscillator**

- Refer to “hazmat331.pdf) (in I://Customer Service folder) : <..\..\Rubidium oscillators-MSDS - Hazardous material>
- Direct link to this document in Spectratime website: <https://www.oroia.com/sites/default/files/document-files/hazmat331.pdf>

### Rubidium Oscillator Product Safety Data Sheet

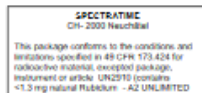
#### 1. Introduction

The following PSDS (Product Safety Data Sheet) contains information which should answer any questions relating to handling/shipping of Rubidium (Rb) oscillators and products containing those oscillators.

#### 2. Radioactivity

This analysis shows a total activity level of less than  $1.6 \times 10^4$  micro-Curie per Rubidium oscillator due to Rb 87. The transportation of RbCl (Rubidium Chloride) in airplane is authorized. However, DOT (Department of Transportation) regulations require that shipping packages be labeled even when the level are within acceptable limit. Shipping documents or shipping containers need to show that the product is safe to handle.

Example of SpectraTime labeling / or shipping documents indications:



#### NOTICE OF NONHAZARDOUS RADIOACTIVE MATERIALS

##### 2.1 ITEM

Frequency Standard: Rubidium

##### 2.2 RADIOACTIVE MATERIAL

$^{87}\text{Rb}$ , specific activity = 0.064 micro-curie/gram

##### 2.3 DECAY MODE

Beta decay, 0.27 MeV

##### 2.4 LOCATION & AMOUNT

The hermetically sealed glass rubidium lamp and cell assemblies each contain a small amount of rubidium metal. The rubidium is a mixture of natural rubidium containing:

73 atom percent of  $^{85}\text{Rb}$

27 atom percent of  $^{87}\text{Rb}$  and separated  $^{87}\text{Rb}$  isotope.

The  $^{87}\text{Rb}$  is mildly radioactive with a half life of  $4.88 \times 10^{10}$  years. The total amount of radioactive rubidium in the frequency standard is <1.3 mg.

##### 2.5 RADIOACTIVE MATERIAL SOURCE

SpectraTime obtains the rubidium from natural sources in the form of RbCl that is a stock item in many retail stores selling chemicals.

[sales@spectratime.com](mailto:sales@spectratime.com)  
[www.spectratime.com](http://www.spectratime.com)

Redwoodland Headquarters  
+41 32 732 85 86

North America Sales Office  
+1 512 471 3880

All OTCs Group 

### Rubidium Oscillator Product Safety Data Sheet

#### 2.6 RUBIDIUM ACTIVITY LEVEL

Our calculations are based on the entire rubidium content being the most active  $^{87}\text{Rb}$  so that the calculation is conservative and reflects a highest level possible. The total level of both cells combined would be less than  $1.6 \times 10^4$  micro-curies.

#### 2.7 EXEMPT FROM LICENSE

Since the used rubidium is a natural-occurring substance and the amount is less than 1 gram, neither the State of Arizona nor the NRC requires a license to manufacture or distribute this product.

#### 2.8 TRANSPORTATION

The U.S. Department of Transportation under 49 CFR 173.424 allows for the unrestricted shipment of instruments containing rubidium conforming to the requirements of Table 7. Rubidium oscillators manufactured by SpectraTime are in conformance with the said Table and required limitations of the code.

### 3. Other Hazards Related to Rubidium Non-Radioactive Properties

#### 3.1 DURING NORMAL OPERATION OF RUBIDIUM OSCILLATORS

No hazard

#### 3.2 IN CASE OF RUBIDIUM RELEASE (GLASS CELL FAILURE)

Despite the very reactive and corrosive properties of Rubidium, the limited amount of material (< 1.3 mg, < 1 mm<sup>3</sup>) contained in the oscillators does not present any hazard.

Nevertheless the following basic precaution must be taken in case of Rubidium release following a glass cell rupture:

- Do not inhale or ingest, and avoid contact with the skin and the eyes.
- Keep away from foodstuff, beverages and feed
- Wear gloves and pick-up mechanically.
- In case of contact with eyes, rinse immediately with plenty of water

#### 4. Disposal

Material should be disposed in accordance with local, state and federal or national regulations.

[sales@spectratime.com](mailto:sales@spectratime.com)  
[www.spectratime.com](http://www.spectratime.com)

Redwoodland Headquarters  
+41 32 732 85 86

North America Sales Office  
+1 512 471 3880

Page 2 of 2

All OTCs Group 

**2.4 LOCATION & AMOUNT (of Rb material):** The hermetically sealed glass rubidium lamp and cell assemblies each contain a small amount of rubidium metal. The rubidium is a mixture of natural rubidium containing:

73 atom percent of  $^{85}\text{Rb}$

27 atom percent of  $^{87}\text{Rb}$  and separated  $^{87}\text{Rb}$  isotope.

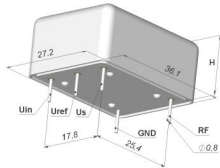
The  $^{87}\text{Rb}$  is mildly radioactive with a half life of  $4.88 \times 10^{10}$  years. The total amount of radioactive rubidium in the frequency standard is <1.3 mg

---

3) **HP (high Performance) Low phase noise OCXO oscillator (LPN OCXO) (P/N: SecureSync- x2y, such as SecureSync-021, SecureSync-023 or SecureSync-027 for examples )**

**Note:** Low phase noise oscillator is not available with the Models 9483 and 9489

- Displayed in browser as: “**OCXO (1PPB)**”
- Used by itself or combined with Rb osc for the low phase noise Rb configuration
- MFG info for low phase noise OCXO
  - **Our P/N:** Y100R-0002-PH10
  - **MFG:** Morion Inc (in Saint-Petersburg, Russia) <http://www.morion.com.ru/>
  - **Model** XO01273M (made-to-specs for Spectracom. Per Arena, appears it's a mod of the MV-197 OCXO but its not labelled as MV-197)



- **Description:** OCXO,TH,10MHz,12V,1PPB,EURO,-20C,90C, Low Aging
- Data sheet also in Arena:
  - **In Arena at:** [https://app.bom.com/items/detail-sourcing?item\\_id=1202848068&version\\_id=10228404878&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqn\\_o=7252161677](https://app.bom.com/items/detail-sourcing?item_id=1202848068&version_id=10228404878&orb_msg_single_search_p=1&redirect_seqn_o=7252161677)

**Note from Dave Sohn:** The low phase noise MV197 is marked **XO01273M**.

- Using this LPN oscillator with a 5MHz (1204-08) or 1MHz (1204-26) output card
- Note this LPN oscillator provides low phase noise 10 MHz outputs (as specified in the SecureSync data sheet) for the base output and 1204-1C 10MHz Option Cards. But these same 10MHz specs DO NOT apply to the 5 MHz or 1MHz outputs. Because of the way these other signals are derived, their phase noise is inherently higher.

---

4) **Standard OCXO oscillator for SecureSyncs only (not NetClocks) (PN: SecureSync- x1y such as SecureSync-011 or SecureSync-013 for examples)**

- Displayed in browser as: “**OCXO (5ppb)**”
- **Our P/N:** Y100R-0002-PH05
- **MFG:** Morion Inc (in Saint-Petersburg, Russia) <http://www.morion.com.ru/>
- **MFG P/N** X000980M Rev 2 (it's apparently a MV-197 made-to-specs for Spectracom)
- **Description:** VCOCXO,TH,10MHz,12V,5PPB,EUROPK,-20C,90C
- **Part is labeled as “MV-197”**
- **in Arena at:** [https://app.bom.com/items/detail-spec?item\\_id=1202848066&version\\_id=10228404838](https://app.bom.com/items/detail-spec?item_id=1202848066&version_id=10228404838)

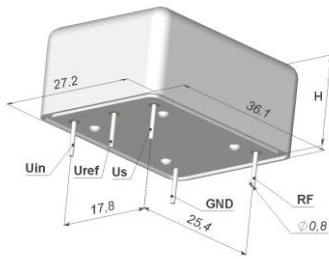
---

5) **Standard OCXO oscillator for NetClock 9483 only (not SecureSyncs)**

- Displayed in browser as: “OCXO (5ppb)”
- Option 5 in Models 9483 and 9489

- **Our P/N:** Y100R-0002-PH03
- **MFG:** Morion Inc (in Saint-Petersburg, Russia) <http://www.morion.com.ru/>

**Mfg P/N:** MV197



**Description** VCOCXO, TH, 10MHz, 12V, 5PPB, EUROPK, 0C, 60C

- **in Arena at:** [https://app.bom.com/items/detail-whereused?item\\_id=1202848065&version\\_id=10298209508](https://app.bom.com/items/detail-whereused?item_id=1202848065&version_id=10298209508)

**6) TCXO oscillator (P/N SecureSync- x0y such as SecureSync-001, SecureSync-003 or SecureSync-011 for examples)**

- Available with SecureSync as well as the Models 9483 and 9489
- Displayed in browser as: “??”

**Our P/N for this external oscillator:** Y100R-0002-TS01

**Mfg. P/N:** Refer to Arena link further below

**Description:** VCTCXO, SM, 10.000MHz, 3.3V, 1PPM -40C- 85C, 5x7mm

2. Our Spec sheet:  
<https://files.bom.com/download/tbvAbexlHEgxf4dhx2u5EEJfjz9mWz1z/xrpajljoubsimkfwogqxfhygszqrbfub/Y100R-0002-PH09%20SCD%20Rev%20C.pdf>
3. In **Arena at:** [https://app.bom.com/items/detail-spec?item\\_id=1202848067&version\\_id=10228404868&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=7251889364](https://app.bom.com/items/detail-spec?item_id=1202848067&version_id=10228404868&orb_msg_single_search_p=1&redirect_seqno=7251889364)



---

7) Raytheon AMDR special 1200 LPN, Wenzel g-Compensated Oscillator SecureSync (SecureSync-R563)

**Note:** Raytheon also refers to this product as the “Frequency Time Server” (or the “FTS 1200”)



- For more info on Raytheon AMDR SecureSync special, refer to: <I:\Customer Service\Customers\Raytheon AMDR project>
- See Tim Tetreault for any specifics regarding this special SecureSync master oscillator.

**C) “-2 Config” (2<sup>nd</sup> generation)**

**SecureSync R563,15,06,15,3B,15,00**

SecureSync P/N purchased: **1200-9013-0601 (in Arena):** [https://app.bom.com/items/detail-spec?item\\_id=1228737122&version\\_id=10956131348&](https://app.bom.com/items/detail-spec?item_id=1228737122&version_id=10956131348&)

**D) “-4 Config” (2<sup>nd</sup> generation)**

- Fiber PTP, Single mode fiber (SecureSync R563,15,06,15,3B,15,00)

**SecureSync P/N purchased: 1200-9029-0601 (in Arena):** [https://app.bom.com/items/detail-spec?item\\_id=1238722969&version\\_id=10956131378&](https://app.bom.com/items/detail-spec?item_id=1238722969&version_id=10956131378&)

**“Original configuration”**

**SecureSync P/N purchased: 1200-R007-0601 (in Arena)** [https://app.bom.com/items/detail-spec?item\\_id=1204952326&version\\_id=10291838828](https://app.bom.com/items/detail-spec?item_id=1204952326&version_id=10291838828)

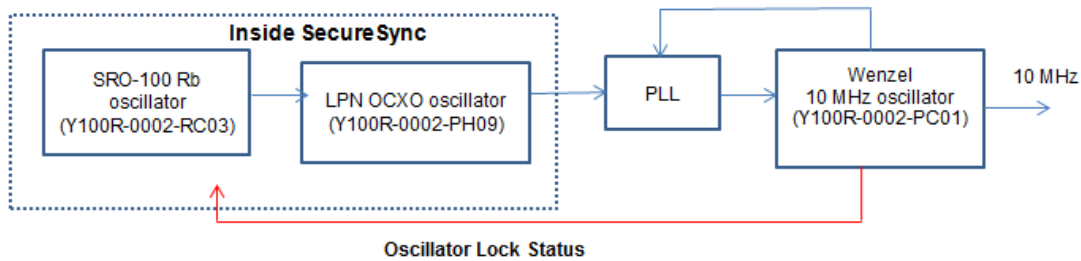
**Has three (3) 10 MHz Oscillators:** Low phase noise 10 MHz in a high G environment on ships

- One (1) internal SpectraTime SRO-100 Rubidium oscillator
- One (1) internal Morian 10 MHz OCXO oscillator
- One (1) External osc from Wenzel that is specialized for High Gs (details for this oscillator below):

➤ **Our P/N for this external 10 MHz oscillator from Wenzel:** Y100R-0002-PC01

- **In Arena at:** [https://app.bom.com/items/detail-attach?item\\_id=1204722998&version\\_id=10245567288&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=7327495950](https://app.bom.com/items/detail-attach?item_id=1204722998&version_id=10245567288&orb_msg_single_search_p=1&redirect_seqno=7327495950)

- VCOCXO,CM,10MHz,12V,5x10-10,5x6x2.75",20C to 35C
- **MFG. P/N** 28056d

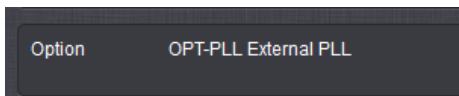


### A. Wenzel Low-G 10 MHz-SC Citrine Crystal Oscillator (Hughes SecureSync, for example)

- P/N: Y100R-0002-PC02 (in PLM) [https://app.bom.com/items/detail-spec?item\\_id=1211979123&version\\_id=10370425508&orb\\_msg\\_single\\_search\\_p=1&redirect\\_seqno=7539269985](https://app.bom.com/items/detail-spec?item_id=1211979123&version_id=10370425508&orb_msg_single_search_p=1&redirect_seqno=7539269985)
- Very low phase noise / low vibration (low G) oscillator for Hughes special SecureSync (refer to “Specials” section in this document for more info on this Hughes SecureSync)
- Internal oscillator (inside the SecureSync chassis)

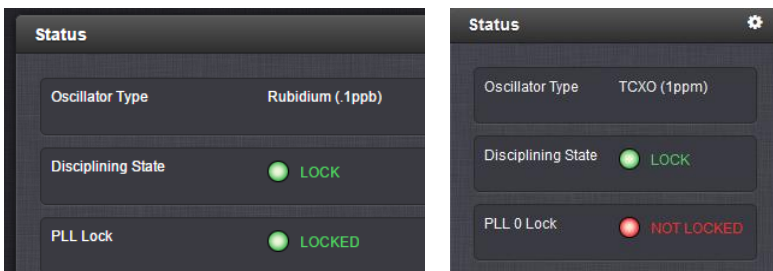
### Lock Status for Raytheon AMDR special SecureSync (our Rb oscillator locking a Wenzel OCXO Oscillator very low phase noise OCXO)

- Referred to as “Opt-PLL External PLL”
- Enabled with license file



- Available starting in version 5.2.1
- Only viewable in the Raytheon AMDR special SecureSyncs (Management -> Disciplining, under “Status”)

**Email from Tim Tetreault (~13 July 2015)** PLL status is available visibly within the web UI on the MANAGEMENT -> Disciplining page under the “Status” section like below.



The PLL status is also rolled up into our frequency error condition, which triggers notifications through our standard mechanisms (UI, logs, SNMP, email, etc.)

**Another email from Tim Tetreault (9/21/2018)** Did we get any background info on this unit from Raytheon? Was it working and then stopped or never worked? Did they give you any logs that we can look at that show the “Lock” status? I think that info was in the System logs.

The “Lock” detect is very straight forward. A Licenses installed in the unit enables it. If the Licenses was not installed, it would not

report any information about the lock.

If we don't see anything in the logs, they might need to send us the units back to fix. Before making that decision, have them answer the questions above.

### Log entries for Wenzel PLL lock status (in osc.log)

- Refer to the CGU manual addendum for Hughes (1200-5000-C050) in Arena at: [https://app.bom.com/items/detail-spec?item\\_id=1217182411&version\\_id=10446313248&orb\\_msg\\_single\\_search\\_p=1](https://app.bom.com/items/detail-spec?item_id=1217182411&version_id=10446313248&orb_msg_single_search_p=1)

PLL\_0 Lock Error (KAD)  
PLL\_0 Lock Good (KAD)  
PLL\_1 Lock Error (KAD)  
PLL\_1 Lock Good (KAD)

### Example entries in osc.log

|    |                 |          |                        |
|----|-----------------|----------|------------------------|
| 91 | Nov 03 00:31:48 | [system] | PLL_1 Lock Error (KAD) |
| 90 | Nov 03 00:31:48 | [system] | PLL_0 Lock Error (KAD) |
| 89 | Nov 03 00:31:30 | [system] | PLL_0 Lock Good (KAD)  |
| 88 | Nov 03 00:30:47 | [system] | PLL_1 Lock Good (KAD)  |
| 85 | Nov 03 00:13:39 | [system] | PLL_1 Lock Error (KAD) |
| 84 | Nov 03 00:09:10 | [system] | PLL_0 Lock Error (KAD) |

**(Non-Wenzel oscillator SecureSyncs) Note PLL\_0 Lock Error (KAD) / PLL\_1 Lock Error (KAD) entries have also been observed on non-wenzel oscillator configuration.**

- In at least case (case **262649**) it appears it can happen if the KTS version isn't the correct version for the CFcard version installed (such as replacing the CF Card without then applying a software update)
- Based on a few other cases (such as 203789 and 284051) it appears these entries can simply be another indication the Rb oscillator is failing/has failed (not meaning anything different).

---

**Issue: glitches in 10 MHz oscillator (typically associated with OCXO) output causes LED time to stop counting up. LCD display is fine.**

- Refer to Mantis case 2916 (except below)

Some SecureSyncs/NetClock 9400s in field are locking up/freezing/losing comms until rebooted.

This was reproduced here with an RMA SecureSync on Burn-in/ Engineering found 10 10 MHz output from the OCXO was missing until unit was rebooted. Apparently, even a momentary glitch in the 10 MHz oscillator output sent to the FPGA can adversely affect the operation of the unit until its rebooted (time on front panel display freezes, sluggish operation, etc).

**All but one unit has an OCXO. The other one has a TCXO.**

- If 10 MHz into FPGA glitches, KTS can't recover without a reboot
- Initial intentions were to add a log entry when it happens and then eventually add a second source of 10MHz into KTS in case the main 10 MHz is temporarily lost.
- As of version 5.2.1, two System log entries are associated with this issue (more info on this below). No fix has been implemented yet to restore operation if it happens (10 MHz input is restored). So if this issue happens, it still won't recover on its own. Power cycle (or possibly reboot) required to restore ops.

**Associated Alarm log entries for loss of 10 MHz**

major alarm ="Timing System Hardware Error".

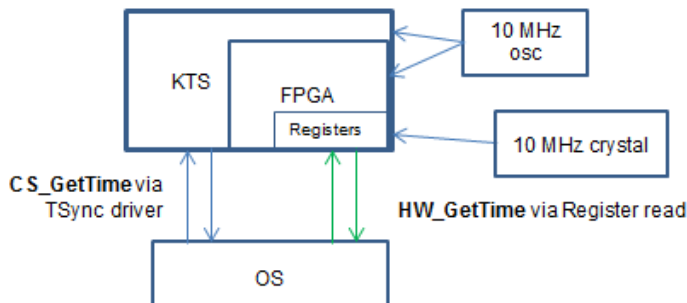
**Associated Kern log entries for loss of 10 MHz (versions 5.2.0 and above)**

- Disabling lock debugging due to kernel taint
- pps pps0: tsyncpci PPS source unregistered
- Spectracom TSync Timing Board removed

**Associated System log entries for loss of 10 MHz (versions 5.2.0 and above)**

- Starting in version 5.2.0, System Log entries will be asserted if the 10 MHz input to the FPGA is lost.
1. Look for the following entries in the System Log
    - Timing System Hardware error
    - Failed CS\_GetTime (KAD)
  2. Then look for either:
    - Passed HW\_GetTime (possible oscillator error) (KAD) OR
    - Failed HW\_GetTime (probably FPGA failure)

**Details**



1. If there are at least five (5) “Failed to read alarm info from KTS (KAD)...” entries in the System log, a “CS\_GetTime” call is sent to KTS to see if KTS is still communicating via the TSync driver.
  - If there are less than 5 entries, nothing happens and the counter is reset
  - If there are at least 5 entries, the Tsync driver **will** be unloaded (reboot will be necessary to restore operation)
  - Associated kern.log entries for driver unloading:
    - pps pps0: tsyncpci PPS source unregistered
    - Spectracom TSync Timing Board removed
2. When a “HW\_GetTime” call is sent to the FPGA registers to see if the FPGA is communicating.
  - If this call passes, the registers are still able to respond (if KTS isn’t running, the same data may remain in the registers). This confirms the TSync driver is still running normally.
  - If this call fails, the registers are not able to provide any data whatsoever. This means either bad FPGA or Tsync driver not running.
3. If both time calls fails, the issue could be with the TSync driver, so it’s unloaded (and remains unloaded) to allow the Network Processor to continue working. Reloading the Tsync driver requires the unit be rebooted.
4. If both calls fail, the oscillator likely glitched, causing both FPGA and KTS to stop responding.
5. If CS\_GetTime fails but HW\_GetTime passes, FPGA is still working.

---

## Oscillator associated alarms not specific to oscillator type

### \*Frequency Error alarm

- Asserted at every boot-up
- Also associated with HUGHES CGU (PLL1 or PLL2)- refer to the Hughes CGU special in this doc.
- Frequency Error is NOT due to the size of the frequency error
- **Per Dave Sohn (2 Dec 2020)** The frequency alarm is related to the DAC as a frequency control alarm that is set if we get within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values.

**Email Dave L sent (8 Dec 2020)** The jump in the oscillator frequency may not trigger a Frequency Alarm.

In the Securesync, the frequency alarm is generated when the DAC which controls the oscillator frequency gets within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values shown in the oscillator log.

To trigger an alarm if the phase error exceeds a certain threshold, the user could set a “Max TFOM for Sync” value which will automatically switch the Securesync to Holdover mode if a certain phase error values is exceeded. The Holdover event will trigger alarms from the Securesync.

Here is the section of the User Manual with more information:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/OscConfiguring.htm?](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm?)

Q ...They experienced the RES-SMT-GG 1.0.9 timing glitch in a 5.8.2 SecureSync, resulting in a suddenly very large

Phase Error. Smart validation/"MaxTFOM lower than 15" weren't being used at the time. Partha wants to know why there were no alerts to the large Phase Errors.

The logs bundle is attached to the Salesforce Case. But the specific observation I'm questioning is why the Frequency Error alarm wasn't asserted, when the Phase Error jump occurred??

Osc.log.1 shows when the timing glitch occurred on 24 Nov

```
Nov 24 16:36:01 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:36:01 000 XO1: Freq error: phase start: +2.6 ns, phase end: +4961.4 ns
Nov 24 16:36:01 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:36:01 000 XO1: Frequency error recalculated: -00.050196 (-5.019x10^-09)
Nov 24 16:36:34 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:36:34 000 XO1: Freq error: phase start: +4961.4 ns, phase end: +7420.4 ns
Nov 24 16:36:34 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:36:34 000 XO1: Frequency error recalculated: 00.001515 (1.515x10^-10)
Nov 24 16:52:43 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:52:43 000 XO1: Freq error: phase start: +4961.4 ns, phase end: +56437.6 ns
Nov 24 16:52:43 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:52:43 000 XO1: Frequency error recalculated: -00.497478 (-4.974x10^-08)
Nov 24 16:53:13 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:53:13 000 XO1: Freq error: phase start: +56437.6 ns, phase end: +57911.6 ns
Nov 24 16:53:13 car-apr-gps3 car-apr-gps3: [system] 2020 329 16:53:13 000 XO1: Frequency error recalculated: 00.001666 (1.666x10^-10)
Nov 24 17:09:43 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:09:43 000 XO1: Freq error: phase start: +56437.6 ns, phase end: +106799.4 ns
Nov 24 17:09:43 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:09:43 000 XO1: Frequency error recalculated: -00.493818 (-4.938x10^-08)
Nov 24 17:10:13 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:10:13 000 XO1: Freq error: phase start: +106799.4 ns, phase end: +108286.5 ns
Nov 24 17:10:13 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:10:13 000 XO1: Frequency error recalculated: 00.001666 (1.666x10^-10)
Nov 24 17:26:43 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:26:43 000 XO1: Freq error: phase start: +106799.4 ns, phase end: +157174.1 ns
Nov 24 17:26:43 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:26:43 000 XO1: Frequency error recalculated: -00.493853 (-4.938x10^-08)
Nov 24 17:27:13 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:27:13 000 XO1: Freq error: phase start: +157174.1 ns, phase end: +158660.1 ns
Nov 24 17:27:13 car-apr-gps3 car-apr-gps3: [system] 2020 329 17:27:13 000 XO1: Frequency error recalculated: 00.001666 (1.666x10^-10)
```

But there were no alarms asserted on 24 Nov (last entry in log was from a reboot, back in June)

```
May 21 21:10:38 car-apr-gps3 car-apr-gps3: [system] ACTIVE ALARMS: NONE
Jun 1 22:02:09 car-apr-gps3 car-apr-gps3: [system] ACTIVE ALARMS: MAJOR MINOR
Jun 1 22:02:18 car-apr-gps3 car-apr-gps3: [system] ACTIVE ALARMS: MAJOR
Jun 1 22:02:21 car-apr-gps3 car-apr-gps3: [system] Frequency Error
Jun 1 22:02:21 car-apr-gps3 car-apr-gps3: [system] ACTIVE ALARMS: MAJOR
Jun 1 22:08:11 car-apr-gps3 car-apr-gps3: [system] ACTIVE ALARMS: NONE
Jun 1 22:08:11 car-apr-gps3 car-apr-gps3: [system] STATUS CHANGE:
Jun 1 22:08:11 car-apr-gps3 car-apr-gps3: [system] ~~~~~ (last entry in log)
```

probably something simple I'm missing. But shouldn't the Frequency Error alarm have been asserted on 24 Nov at about 16:36 UTC (even if its masked, it should've been logged)??

**A Email from Dave Sohn (2 Dec 2020)** The frequency alarm is related to the DAC as a frequency control alarm that is set if we get within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values.

**Question from Dave Loerah to Dave Sohn** I had a question about the Frequency Alarm. I was always under the impression the

alarm was generated if the phase error exceeded a certain threshold. If that is not the case, how would the customer know if the phase error was very high and their timing quality was compromised?  
I have a customer report they had a high phase error jump and there were no alarms.

**Reply from Dave Sohn (8 dec 2020)** The frequency error is related to the DAC value approaching our frequency control limits. Phase error reporting would be through the maxTFOM settings.

---

## **\*\*Rubidium oscillator-associated alarms**

- Also refer to: “SRO-100 Rubidium oscillators” in the Customerserviceassistance document

### **Alarms associated with likely hardware failure of Rb oscillator**

- Are there “**Rb lamp error**”, “**Rb peak voltage error**” or “**Rb fault detected**” messages in the Timing Log? This will indicate a failed Rubidium oscillator module.

#### **1) Rb Peak voltage error**

**Note:** Archive software versions 5.0.0 and below reported all alarms associated with the Rubidium oscillator as “**Rb peak voltage error**” alarms. This was noticed just prior to the version 5.0.1 release, so version 5.0.1 now differentiates each Rb oscillator alarm to indicate what the real issue with the Rb oscillator.

Q. (log entry from Morgan Stanley Rb-based SecureSync) **Rb peak voltage error** (val=6, min=51, max=255)

**A (1/25/12) Mark Goodlein emailed SpectraTime with:** We have a customer with one of our SecureSync products, in which we use an SRO-100 Rubidium oscillator module. Recently, this customer saw some behavior that was questionable and would like to know if they should be concerned about it.

Our software that communicates with the SRO requests the internal parameters using the ‘M’ command once a second. It then compares the values returned with boundary values to detect if something is out of the ordinary, in which case we log the condition. This customers unit had been running for over 150 days then the following log messages were recorded for 5 seconds then went away and no more have been logged since then.

```
2011 357 21:26:54 000 Rb peak voltage error (val=6, min=51, max=255)
2011 357 21:26:55 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:56 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:57 000 Rb peak voltage error (val=9, min=51, max=255)
2011 357 21:26:58 000 Rb peak voltage error (val=35, min=51, max=255)
```

The manual for the SRO indicates that this signal stabilizes to between 1 and 5 volts after warm-up, so these are the boundary conditions that our software checks for. In this case, the voltage dipped below 1V (almost reaching 0V) for 5 seconds. This is the first case of an event like this that has ever been reported to us from a customer.

Is this event something to be concerned about? Does it indicate a condition that may result in failure?

---

## **\*\*Oscillator free-run/Holdover specs**

- Refer to SecureSync data sheet for most recent oscillator specs (“SecureSync 3 page”):

*From the SecureSync user manual*

| Oscillator Type               | Typical Error Rates after 4 hrs | Typical Error Rates after 24 hrs |
|-------------------------------|---------------------------------|----------------------------------|
| Low Phase noise Rb (Rubidium) | 0.2 $\mu$ s (nominal)           | 1 $\mu$ s (nominal)              |
| Rb (Rubidium)                 | 0.2 $\mu$ s (nominal)           | 1 $\mu$ s (nominal)              |
| High performance OCXO         | 0.5 $\mu$ s (nominal)           | 10 $\mu$ s (nominal)             |
| Standard OCXO                 | 1 $\mu$ s (nominal)             | 25 $\mu$ s (nominal)             |
| TXCO                          | 12 $\mu$ s (nominal)            | 450 $\mu$ s (nominal)            |

**Table 3-3:** Estimated oscillator error rates during Holdover

From the SecureSync data sheet

**Holdover** (constant temp after 2 weeks of GPS lock)

|                         | TCXO (nominal)                       | OCXO (nominal)   | Low Phase Noise OCXO (nominal) | Rubidium (nominal) | Low Phase Noise Rubidium (nominal) |
|-------------------------|--------------------------------------|------------------|--------------------------------|--------------------|------------------------------------|
| After 4 hours           | 12 microseconds                      | 1 microsecond    | 0.5 microseconds               | 0.2 microseconds   | 0.2 microseconds                   |
| After 24 hours          | 450 microseconds                     | 25 microseconds  | 10 microseconds                | 1 microsecond      | 1 microsecond                      |
| after 7 days            | 3150 microseconds (3.1 milliseconds) | 175 microseconds | 70 microseconds                | 7 microseconds     | 7 microseconds                     |
| after 30 days (nominal) | 13,950 microseconds                  | 775 microseconds | 310 microseconds               | 31 microseconds    | 31 microseconds                    |

**Important Note:** The 1PPS drift is not linear. It ramps up, as the oscillator ages. You can't just multiply the numbers above by the desired amount of lapsed time to determine how far off it will be. Dave Sohn has a Model they use to calculate time drift over a given amount of time.

**Link to Engineering's simulated OCXO/TCXO oscillator drift graphs over an extended periods of time:**  
<I:\Engineering\1PPS drift simulations for various Spectracom oscillators>

### A) Low phase noise OCXO Oscillators

(From Dave Sohn) Estimate for low phase noise OCXO holdover at constant temperature (after 2 weeks with GPS lock)

| Days | Drift  |
|------|--------|
| 1    | 10 us  |
| 2    | 40 us  |
| 3    | 80 us  |
| 7    | 430 us |

### B) Rubidium Oscillators

1PPS holdover estimates for Rubidium oscillators at constant temperature after 2 weeks of GPS lock



| Days | 1PPS Phase Error |
|------|------------------|
| 1    | 2us              |
| 7    | 11us             |
| 14   | 30us             |
| 30   | 95us             |

Here are results if you had a temperature change of 10 degrees C at a rate of 1 degree per hour over the same holdover time periods.

| Days | 1PPS Phase Error |
|------|------------------|
| 1    | 3us              |
| 7    | 25us             |
| 14   | 55us             |

---

### Sonet/Telecom Stratum hierarchy levels for 1544/2048 kHz, T1/DS1 and E1 outputs

- Such as Stratum 1 and Stratum 3E
- Refer to “Stratum timing for 1544/2048 kHz, T1/DS1 and E1 outputs” in the T1/E1 section of the SecureSync Option Card info document for more info.

---

### OCXO comparison chart

- The following is a link to a chart which shows accuracy when locked and free run mode:

<I:\Engineering\Products\ProductPerformanceSpecs5.xls>

---

### Holdover for Simulcast specs (time to drift 5 microseconds)

- Per Ed, certain Simulcast systems can tolerate up to **5 microseconds** of 1PPS drift before issues start to happen
  - Customers may ask how long can “Holdover timeout be set to. while maintaining less than 5 microseconds of drift (refer to Salesforce Case 177534)
  - Ed’s recommendations are to set Holdover to **5 days for a Rubidium oscillator or 5 hours with an OCXO**

---

### \*\*Oscillator warm-up/stabilization (time to warm up to operating temperature)

#### A) Rb oscillator

- At least three days recommended for full warm-up and for the oscillator to stabilize.

**Note:** (software issue applicable to versions 5.8.4 and below – fixed in 5.8.5) refer to “**RB oscillator potentially stuck in warm-up mode**” further below in this document

#### B) OCXO oscillator

### **C) TCXO oscillator**

- Not applicable: TCXO oscillator is not an ovenized oscillator.

---

## **\*\*Oscillator Calibration (Hertz range/DAC values)/recalibrate checkbox**

### **Oscillator DAC value**

#### **Desire to obtain the current DAC value**

- Refer to Salesforce Case 267494 (excerpt email further below)

#### **Current DAC value available via:**

- "Unsupported" CLI call: **XO\_GetDac 0**<enter>.
- **Management** -> **Disciplining** page of browser
- REST API interface
- Oscillator log
- Log bundle (sqlite database data) ??

#### **Doesn't appear to be available via (as of at least v5.9.1)**

- Front panel display
- SNMP get

Note the **DAC** values in the **Oscillator** log entries and in **XO\_GetDac 0** CLI call are reported as hex values ("0x"). Convert the hex value to decimal value, via an Internet converter, such as:

<https://www.rapidtables.com/convert/number/hex-to-decimal.html?x=D555>

**Email from Keith to a customer 24 June 2021)** In addition to the DAC value being available via the web browser (as well as the associated REST API interface that the browser supports), the DAC value appears to only be available via one "unsupported" CLI call. The list of supported CLI calls is available in the online SecureSync user guide at [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/APPENDIX/CLICommands.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/APPENDIX/CLICommands.htm). But there are other unsupported "get" calls also available.

With a telnet/ssh connection to the SecureSync, the associated CLI call (as shown below) to obtain the DAC value, as a hex number) is **XO\_GetDac 0**<enter>.

```
spadmin@Spectracom ~ $ XO_GetDac 0
DAC value: 0x7F7F
spadmin@Spectracom ~ $ █
```

It doesn't appear the DAC value is available via the front panel LCD display (the "closest" selection is Status. But as you mentioned, Status doesn't report the DAC). So the choices to obtain the DAC are the web browser, REST API and CLI interface. I thought it MIGHT also be available via SNMP. But I just checked the MIBs and don't see it being available.

---

## Oscillator Calibration

### A) Rb Oscillator Calibration

- The calibration value is set during initial factory testing and not every time the Securesync is rebooted.
  - This sets the frequency range values for the particular oscillator installed and from then on, the oscillator self-calibrates.
  - The final verification test does not require any calibration. It checks to ensure all tests pass and meet specifications.
- The only time these values are changed after initial factory test is when a Manual Recalibration is performed. When the customer recalibrates the oscillator, it will provide fresh cal values so the oscillator can be precisely adjusted.

### Questions

1. Does the calibration value mean frequency value of stable rubidium?
2. Is the calibration value determined every boot up and recalibration process?

**Email from Dave L (18 June 20)** The oscillator is controlled by software steering a Digital to Analog Converter IC. The DAC sends a control voltage to the oscillator.

The Oscillator calibration process will set the DAC to its highest adjustment rail, then to the lowest adjustment rail. The difference in the oscillator frequencies of each setting is used to compute the total adjustment range of the oscillator. This frequency range value is used to optimally control the oscillator. If incorrect or erroneous calibration values are saved in the configs the software disciplining algorithm has trouble making precise adjustments to the oscillator.

The calibration value is set during initial factory testing and not every time the Securesync is rebooted. The only time these values are changed after initial factory test is when a Manual Recalibration is performed. When the customer recalibrates the oscillator it will provide fresh cal values so the oscillator can be precisely adjusted.

If this does not resolve the problem for some reason the oscillator must be faulty and we will need to arrange a RMA.

---

### B) TCXO/OCXO oscillator calibration

- TCXO/OXCXO oscillators are calibrated first time they are powered-up/synced. This cal data is then stored in a file in the EPROM

#### Two types of “H/S’ cal data logs are asserted into the Oscillator logs:

- “Saved Cal Value”: the previous calculated value stored in the EEPROM
- “New Cal Value”: only happens at factory, or if a patch is applied to reset it. This entry can be eventually overwritten by other, more recent entries

**Typical “H/S” cal values (from a standard OCXO oscillator) as obtained by searching an Oscillator log for “H/S” entries**

| <b>Id</b> | <b>Date</b>     | <b>Entity</b> | <b>Message</b>                                                |
|-----------|-----------------|---------------|---------------------------------------------------------------|
| 510       | Jul 11 18:32:32 | [system]      | 2014 192 18:32:32 000 XO1: New Cal Value: H/S:+0.0001377126   |
| 503       | Feb 03 17:42:53 | [system]      | 2014 192 17:42:39 000 XO1: New Cal Value: H/S:+0.0001374532   |
| 498       | Jul 08 21:19:14 | [system]      | 2014 189 21:19:14 000 XO1: Saved Cal Value: H/S:+0.0001537346 |
| 475       | Jul 03 13:11:11 | [system]      | 2014 184 13:11:11 000 XO1: Saved Cal Value: H/S:+0.0001537346 |
| 12        | Jun 27 21:26:12 | [system]      | 2014 178 21:26:13 000 XO1: Saved Cal Value: H/S:+0.0001537346 |

**Oscillator Calibration log entries (*Tools* -> *Logs* page of the browser, *Oscillator* tab)**

Starting in version 4.8.6 (June 2012) Oscillator calibration value (which is stored in EEPROM during manufacturing) are reported in the Oscillator log after every power-up.

**Example log entries below:**

**1. Valid / expected log entries**

Jun 29 16:07:02 Spectracom spectracom: [system] 2012 181 16:07:02 000 Saved Cal Value: **H/S:+0.000150**  
Jun 29 16:07:02 Spectracom spectracom: [system] 2012 181 16:07:02 000 Initial DAC Setting: 0x8639  
Jun 29 16:04:29 Spectracom spectracom: [system] 2012 181 16:04:29 000 New DAC Setting: 0x863D  
Jun 29 16:03:39 Spectracom spectracom: [system] 2012 181 16:03:39 000 New DAC Setting: 0x8630  
Jun 29 16:02:49 Spectracom spectracom: [system] 2012 181 16:02:49 000 New DAC Setting: 0x8635

**2. Bad / invalid log entries**

Jun 27 21:41:07 Spectracom spectracom: [system] 2012 179 21:41:06 000 New DAC Setting: 0xFFFF  
Jun 27 21:39:08 Spectracom spectracom: [system] 2012 179 21:39:07 000 Saved Cal Value: **H/S:+0.000000**  
Jun 27 21:39:08 Spectracom spectracom: [system] 2012 179 21:39:07 000 Initial DAC Setting: 0xA670  
Jun 27 21:18:39 Spectracom spectracom: [system] 2012 179 21:18:39 000 Frequency error recalculated: 05.112250

**Note:** H/S value should not be displayed as all 0's. This indicates a bad calibration occurred. Oscillator Alarm will likely be asserted in the Alarms log. Cal needs to be set to all 0.s which will cause the calibration to be re-performed.

**Resolution for this known potential issue with 4.8.9 having bad cal data out of the box**

- Refer to Michael Cribbs, Salesforce case 11202
- Symptoms are not syncing to GPS (even with good reception) much higher TFOM than usual, and oscillator log containing entry of “XO1: New Cal Value: H/S:+0.0000000000.
- Flag record as out of box failure.
- Fixes are to **Version 5.2.0**- Perform a “Recalibrate” (*Management* - > *Disciplining* page).

---

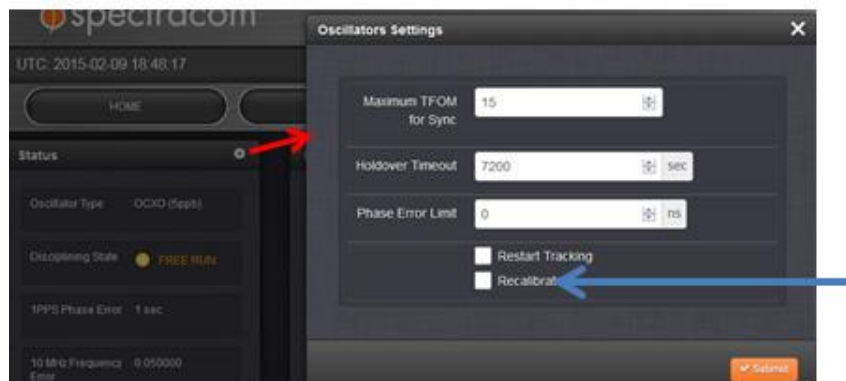
## Oscillator recalibration (Recalibrate checkbox)

### TCXO/OCXO oscillator recalibrate in the field (BAD/questionable oscillator calibration/Recalibrate checkbox)

- Refer to the Word document in the folder: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Recalibrate a TCXO or OCXO osc](#)

#### A) Versions 5.2.0 and above (“Recalibrate” checkbox is available)

- For TCXO/OCXO oscillators only
- Update version 5.2.0 added a “Recalibrate” checkbox to the newer browser (not available in classic interface). Refer to Mantis case 1731.
- This checkbox (**Management** -> **Disciplining** page of the browser) allows the oscillator to be recalibrated by a customer without the need to run a patch or login as spfactory mode.
  - **Note:** This checkbox sends the following newer CLI command: **XO\_SetMode 0 3** to recal the oscillator.



- If a bad oscillator calibration happens to occurs, it won't run the cal again:
- With Software versions 5.2.0 and above, can perform a “Recalibrate”
- Make sure SecureSync is in full sync (not Holdover) with a good 1PPS referene (such as GPS or IRIG from a very stable generator).

#### “Recalibrate” button with a Rubidium or Low phase noise Rubidium oscillator

- Recalibrate button shouldn't have any effect on a standard rubidium unit
- Low Phase Noise Rubidium consists of an OCXO that locks to a standard Rubidium after each boot-up. This button shouldn't affect the Rb oscillator lock, but will affect the OCXO lock to the Rubidium oscillator, until the SecureSync is rebooted again. If the recalibrate button is pressed, reboot the SecureSync to restore OCXO lock to the standard Rb oscillator.

---

#### B) Versions 5.1.7 and below (the “Recalibrate: checkbox is not available)

- For TCXO/OCXO oscillators only
- Requires remote access to the spfactory account.
- If a bad occurs requires an EEPROM patch update file (patch\_img.bin) be uploaded by a customer, Then we need to remote ssh in to issue a command that applies the patch. Then the unit can be rebooted.
  - With Software versions 5.1.7 and below, the cal value needs to be deleted while logged in as root or spfactory. Then, the cal process is performed again, once the system boots again (might be able to

---

remotely access the unit here for our Engineering team to reset the value for them

### C) Versions 5.1.7 and below:

- 1) Update to 5.2.0 and then perform a "Recalibrate"(Management - > Disciplining page).
- 2) Return it to us
- 3) An engineer to remote login as root,
- 4) Or best method for field fix – either upgrade to v5.0.0 or higher (Not downgrade to 4.8.8 and clean and then upgrade back to 4.8.9 anytime thereafter). If they update to 5.0.0 or higher, it will cal the oscillator after getting valid GPS input.

Note that it's much easier to upgrade to v5.x.x than to downgrade to 4.8.8, because you don't have to clean, and alleviates the need to upgrade back to 4.8.9 anytime thereafter.

H/S being all 0's with units that shipped with 4.8.9 is a potential issue that can occur. It will cause higher than expected TFOM (such as 10) and trouble syncing, even with good GPS.

Per the draft email for this condition (also below in red), besides an engineer logging remotely into root, or needing for it to be sent back to us for re-cal, the best fix in the field is to downgrade from 4.8.9 to 4.8.8, perform a clean configs (which erases the cal value from the file) let it sync back up for a couple of hours. Then it can be upgraded back to v4.8.9 anytime thereafter (the cal value persists through normal upgrades, but is reset on a clean.

FYI- during the Manufacturing process, a one-time self-calibration of the oscillator is performed to determine its individual Hertz Range for disciplining purposes. Due to a step that was performed in manufacturing, the cal data was inadvertently lost just prior to shipment. So the unit currently has a Hertz Range of 0, which is adversely affecting the oscillator disciplining and its ability to lock/declare sync to GPS (as you are observing).

We can assign an RMA Number for the NetClock to be returned for this self-cal to be performed again, if you prefer. However, with just a software downgrade and then a software upgrade, this process can also be performed in the field, without the need to return it to us. Downgrading it from version 4.8.9 to 4.8.8 and letting it run for a couple of hours will allow the oscillator to be re-calibrated. Anytime thereafter, it can be upgraded back to 4.8.9 again, with this issue resolved.

If you prefer to send it back to us, let me know and I will assign an RMA Number for it to be returned to us for the recal. But in case you would rather not have to return it and want to perform the software "upgrade" process, I have attached the version 4.8.8 upgrade instructions and here is a link to download the version 4.8.8 upgrade file:  
<https://www.dropbox.com/s/hm87jogciba0ij/update488.tar.gz>.

Downgrading to version 4.8.8 is the same as upgrading to any newer version, with the exception that you just need to check the "Force Upgrade" button during the update, in addition to the "Update Firmware" checkbox. The Force update just overrides the version check that normally occurs during upgrades. Once the NetClock has been Force "upgraded" to version 4.8.8, it should be "cleaned" back to the factory default settings (via the Tools-> Upgrade/Backup page of the browser). If you like, the settings can be backed-up off the box and then restored, once it's been updated back to version 4.8.9. Let me know if you would like to do this, instead of reprogramming it.

After downgrading to version 4.8.8, let it sync up to GPS again and then just let it run for at least a couple of hours for the oscillator to settle out and automatically perform its cal.

You will notice the reported TFOM value (as indicated in the **Status -> Time and Frequency** page of the web browser) will go to a much lower value. Go to the Tools -> Logs page and select the Oscillator log. You should see an entry similar (but not likely exactly the same) as the one below. The highlighted/enlarged portion indicates a good oscillator cal has been performed.  
Jun 29 16:07:02 Spectracom spectracom: [system] 2012 181 16:07:02 000 **Saved Cal Value: H/S:+0.000150**

Then, it can be upgraded back to version 4.8.9, using the same update process (upgrades don't need the "Force" box checked, but it doesn't hurt anything if it is checked) and using a version 4.8.9 upgrade file, instead. The version 4.8.9 upgrade file is on our website and can be downloaded at:  
<http://www.spectracomcorp.com/Support/HowCanWeHelpYou/Software/9400NetClockSoftware/tabid/1511/Default.aspx>

Please let me know how you would like to proceed or if you have any questions pertaining to this info!

---

## **\*\*Oscillator Disciplining (RB/OCXO/TCXO)**

### **A) STANDARD Rubidium oscillator disciplining**

**Note:** LPN RB oscillator info further below

#### **Software changes related to Rb oscillator disciplining**

##### **1) Standard Rubidium oscillator disciplining/need to apply a special EPROM patch (“updateRbDisc.tar.gz”) patch when downgrading software version**

Due to a change to newer method of RB oscillator disciplining in 5.8.0 (KTS disciplining the oscillator), a special EPROM patch (“**updateRbDisc.tar.gz**”) file needs to be applied to switch the Rb oscillator to start using the earlier method of disciplining (its own internal disciplining). Until the patch is applied, the oscillator will remain always in a free-run state.

- **Link to updateRbDisc.tar.gz:** [file:///C:/Customer Service/EQUIPMENT/SPECTRACOM/EQUIPMENT/SecureSync/Specials/software patches/Downgrade Rb patch \(updateRbDisc.tar.gz\)](file:///C:/Customer%20Service/EQUIPMENT/SPECTRACOM/EQUIPMENT/SecureSync/Specials/software%20patches/Downgrade%20Rb%20patch%20(updateRbDisc.tar.gz))

#### **1. Software version 5.8.0**

- Changed STANDARD RB odsc disciplining, from Rb disciplining itself to using the same algorithm as OCXO/TCO (KTS disciplining)
  - **(5.8.0 and above) “xo1” now being annotated in Rb osc log entries:** Rb is disciplined using KTS (ike OCXO and TCXO log entries have always been)
  - Example entry with KTS disciplining (v5.8.0 and above)

Jun 19 07:11:04 [system] 2015 170 07:11:04 000 **XO1**: Frequency error recalculated: -00.000332 (-3.328x10<sup>-12</sup>)

- **(5.7.x and below) “xos” was annotated in Rb osc log entries = indicates original disciplining** (Rb disciplines itself in 5.7.x and below)
- Example entry with Rb disciplining itself from (v5.7.x and below)

Apr 29 15:56:14: [system] 2018 119 15:56:13 000 **XOS**: Frequency error recalculated: -00.000005 (-5.194x10<sup>-13</sup>)

#### **Downgrading a Rubidium unit from 5.8.0 (or above) back to 5.7.x and below (newer disciplining algorithms back to original disciplining)/need to install a rb patch**

- Refer to Salesforce Case 180207
- Its **not** recommended to downgrade Rb units back to 5.7.x or below, once they are at a more recent version.
- but if the software is downgraded and a Rb is installed, a special patch file has to be installed- to switch the EPROM back to the original disciplining
- symptoms of downgrading software without the patch being applied includes TFOM values higher than expected (oscillator will be in constant free-run).
- in case 180207, algorithms changed correctly going forward from 5.7 to 5.8.2 But the EEPROM does not change back to the original disciplining of the Rb, when its downgraded (the oscillator stayed with the new method, but the earlier version of software soft) -so the oscillator wasn't properly disciplining after the downgradde. It was instead ramping off.
- To downgrade the disciing back to Rb disciplining itself requires the EEPROM be reprogrammed at the factory (in the field- EEPROM can go forward to KTS discipling but it cant go back to the Rb disciplining itself once its using KTS disciplining. until the patch is applied)
  - This patch file (and draft email) is located at: [file:///C:/Customer Service/EQUIPMENT/SPECTRACOM/EQUIPMENT/SecureSync/Oscillators, rb material/oscillator disciplining/downgrade Rb patch](file:///C:/Customer%20Service/EQUIPMENT/SPECTRACOM/EQUIPMENT/SecureSync/Oscillators_rb%20material/oscillator%20disciplining/downgrade%20Rb%20patch)

#### **2. Software version 5.7.3**



- **Updated disciplining algorithms to improve short term stability and increase the maximum of the dynamic loop constants (not sure if this was Rb and/or OCXO/TCXO)**
  - Changed Rubidium disciplining to operate using common disciplining algorithm with other oscillators for new and existing fielded units. In order to downgrade SW, existing Rubidium units will need to be patched back to previous disciplining mode.

---

## B) Low Phase Noise LPN Rb oscillator (Both RB and OCXO oscillators installed)

### All software versions

- “XOS” = Rb oscillator disciplining
- “XO1” = OCXO disciplining

**Per email from Dave Sohn (1 July 2020)** XOS messages are valid for LPN Rb units, as we still use the XOS for the RB communication while the XO1 handles the OCXO installed. These are two oscillator systems, so we have two different disciplining elements running.

---

### Issues with Rb oscillator disciplining (STANDARD and/or LPN Rb)

#### 1) RB oscillator not disciplining (phase errors continue to increase/RB DAC value not changing)

- Refer to Salesforce Case 215423/215424
- Refer to JIRA SSS-765
- Observed in v5.8.4
- Temporary fix is to restart tracking and workaround to automate is to use phase error limit value

**Email Keith sent (8 Jan 2020)** Based on the earlier logs you had provided, I originally thought there may have been an issue related to the receiver itself. But this wouldn't explain what is being observed. Just before sending the earlier logs over to our engineers for their "2<sup>nd</sup> opinion", I noticed this time that the oscillator DAC values for the two units, were staying at a constant value (though the DAC values the two units are staying at aren't identical). I mentioned this observation to the Engineers while passing the logs to them.

As I started suspecting when they responded, this is a symptom of the reason you are seeing the very high phase errors in the two units. They informed me that they have started looking into a peculiar software issue associated with the Rubidium oscillator disciplining, where the oscillator may stop following its intended steering (instead of correcting the phase error, its instead drifting away from the reference).

They suggested performing a temporary work-around, as they further investigate the root cause. The temporary work-around is to manually perform a "Restart Tracking" on both SecureSyncs In addition, the SecureSyncs can be configured to automate a "Restart Tracking" be automatically performed as needed, if it happens to enter into this same abnormal state again. This is via the "phase error limit" feature.

Both the "Restart Tracking" function (which performs a "one time" coarse-adjustment alignment of the oscillator to its selected input, each time its performed – just like what happens after each reboot, but alleviates needing to perform a full reboot) and the phase error limit (which automates a restart tracking if the phase error exceeds this user-configurable value) are described in the **"Configuring the Oscillator"** section of the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/OscConfiguring.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm)

In summary of the user guide: "Restart Tracking" is initiated (and "phase error limit" is configured) in the **Management -> Disciplining** page of the web browser. Then click the ICON just to the right of "Status" (left side of the page) to open a pop-up window, as shown below



Within a few minutes after selecting "Restart Tracking" (and pressing Submit), you should see the Phase Error now be a significantly

lower value. You can optionally set the Phase Error limit to a value which will cause a Restart Tracking to automatically occur again, if the Phase Error happens to exceed this value. Typical phase error values are less than around 100ns to 150ns. Setting this field to a value such as "200" or "250" (nanoseconds) is likely a good value to use, as the Phase Errors shouldn't typically exceed these values, unless a problem has started occurred again with the disciplining..

At your convenience, please let me know that the phase error significantly decreases after performing Restart Tracking. Thereafter, you shouldn't see the phase error limit exceeding the phase error limit value.

I am also flagging your record to let you know once we have a fix to this very peculiar condition!!

## 2) RB oscillator stuck in warm-up mode (applicable to versions 5.8.0 through 5.8.4)

**Summary:** Rubidium oscillators being disciplined by KTS (instead of internally, versions prior to 5.8.0) starting in 5.8.0, can potentially stay in warm-up mode after initial power-on. This causes very high TFOM (such as TFOM 8), from that point forward

- Refer to case 208069 (for Northrop Grumman)
- Refer to JIRA SSS-583
- Applicable to versions 5.8.0 thru 5.8.4 (fixed in 5.8.5)
- Issue fixed in version **5.8.5** (per 5.8.5 Release Notes: "Modified Rubidium disciplining support to prevent breaking from the warm-up state early")

### Previous RB warm-up patch (applicable to versions 5.8.0 through 5.8.4):

- Was sent to Northrop Grumman
- Should no longer be sent out. Customers should instead update to v5.8.5 (or above) instead of using this patch

---

## C) TCXO/OCXO disciplining

### Note

- **"xo1" is annotated in TCXO/OCO Osc log entries:** TCXO/OCXO is disciplined using KTS (like OCXO and TCXO)
- Example entry with KTS disciplining (5.8.0 and above)

Jun 19 07:11:04 Spectracom-Rubicon Spectracom-Rubicon: [system] 2015 170 07:11:04 000  
**XO1: Frequency error recalculated: -00.000332 (-3.328x10<sup>-12</sup>)**

### 1. version 5.7.3

- Updated disciplining algorithms to improve short term stability and increase the maximum of the dynamic loop constants

### 2. verison 5.4A (Harris Only- replaces Harris version 5.2D which was the beta test for these changes resulting from the GPS satellite timing error)

- Changes associated with Rb Holdover/alariming (replaces interim Harris update version 5.2D) "Spectracom performed the GSG 13.7 usec step testing to put Rb oscillator provisioned units into Rb Flywheel" (Forced Holdover mode if a large GPS 1PPS offset is detected).
- Refer to Section 1.8.3 of the Harris SecureSync Rev 19 manual (1200-5000-H050) (excerpted below)

### **GPS Qualification**

*As of June 2016, Harris SecureSync units with Rubidium (Rb) oscillator are equipped with custom functionality that will detect unexpected steps in the GPS 1PPS input signal by monitoring the phase difference between the GPS 1PPS input signal and the 1PPS signal generated by the Rb oscillator.*

*If a step is too large, i.e. it exceeds a threshold 1, this feature will automatically place SecureSync's Rubidium oscillator into a "flywheel" mode by un-locking the oscillator and system 1PPS from the GPS 1PPS input signal. Instead, the now free-running system 1PPS will be fed to SecureSync's 1PPS output port, thus maintaining the integrity of the output signal.*

*The Rb oscillator remains in this override state maintaining an in-specification 1PPS UTC signal until one of the following conditions is met: Either the GPS 1PPS input returns to within the dynamically calculated threshold, or 12.5 minutes transpire, with SecureSync remaining in the override state: At this point SecureSync will enter Holdover mode. Once the Holdover Timeout is reached, SecureSync will exit synchronization and generate a Major Alarm.*

### **3. Software version 5.3.1 added several improvements to TCXO, OCXO and Low Phase Noise Rb oscillator disciplining**

"Improvements to oscillator disciplining (not applicable to Rubidium oscillators), including phase noise improvements during synchronization" (limits DAC changes to help prevent generating phase noise when the DAC changes).

### **4. Software version 5.3.0 added Host disciplining (NTP input disciplines the oscillator) (TCXO, OCXO and Low Phase Noise Rb)**

### **5. Software version 5.2.0 improvements to TCXO/OCXO/Low Phase Noise Rb oscillator disciplining**

A **phase error limit field** was added to the Edit window of the Disciplining page allowing for an automatic disciplining tracking restart, once the phase error limit is exceeded, thus avoiding manual intervention.

### **6. Software version 5.1.7 improvements to TCXO/OCXO/low phase noise Rb oscillator disciplining**

Dave Sohn incorporated several improvements to oscillator disciplining in 5.1.7, such as smaller step sizes and more steps, better phase recovery when a reference is restored, changes to phase error limits, changes to window selection and waiting 20 minutes before adjusting to a 1PPS jump (if a jump occurs in the selected reference PPS and the 1PPS is still misaligned after 20 minutes and in a different window, it assumes its legit and starts correcting for the offset. This was to account for the potential of erroneous 1PPS jumps occurring in the RES-SMT-GG receiver).

It's still unknown (Nov, 2014) if the version 1.07 firmware update (included in software update v5.1.7) for the RES-SMT-GG receiver will inherently prevent the 1PPS from jumping (Trimble indicates they haven't seen the PPS jump. So there were no known intentional changes in 1.0.7 to fix for the PPS from jumping/ But this update may inherently fix this issue.

### **7. Software version 5.1.4 improvements to TCXO/OCXO/low phase noise Rb oscillator disciplining**

**Email from Dave Lorah to Masataka (24 June 2014)** As far as changes between 5.0.2 and 5.1.4, we improved our measurement window adjustments, improved our initial sync time performance, and added adjustable filtering based on input reference error. There would be a difference in the oscillator log measurements due to these changes. The oscillator measurement range should be in the x10-11 to x10-13 range.

---

**\*\*\*\*\*(HST1) Host disciplining of oscillator when NTP or “User set time” is the selected reference**

**Host disciplining (using NTP input to discipline TCXO/OCXO oscillators, versions 5.3.0 and above only)**

**Note: not applicable to Rb oscillators (whether using its own internal disciplining in 5.7.x and below, or KTS disciplining in 5.8.0 and below)- TCXO and OCXOs only (see additional info further below)**

- This is a newer capability which was added in version 5.3.0 (Sept 2015)
- NTP with then be able to discipline the 10 MHz oscillator (potentially clearing the Frequency Error alarm)
- Version 5.4.5 added ability to disable/enable host disciplining (factory default is not enabled)
  - Customers updating to versions 5.4.5 or above for the first time need to enable host disciplining if a TCXO/OCXO is installed and its desired for the Frequency error alarm to be able to clear (not remaining always asserted).

---

**API calls associated with Host Reference (NTP input)**

- Refer to Tim Tetreault’s “cheat sheet” at: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet>
- These API calls are primarily for internal use, but the associated “get” calls are available via the CLI interface (“sets” are not available to either spadmin or user accounts)
- These are examples - additional calls may have since been added

| <b>Host Reference Commands</b> |
|--------------------------------|
| HR_GetLocal                    |
| HR_GetNumInst                  |
| HR_GetRefId                    |
| HR_GetTimeScale                |
| HR_GetValidity                 |
| HR_SetLocal                    |
| HR_SetTime                     |
| HR_SetTimeScale                |
| HR_SetValidity                 |

---

**Use of Host disciplining (NTP input) with Simulcast applications**

**Important note:** Due to the System PPS being moved/adjusted when synced to other NTP servers, it is NOT recommended for Simulcast customers to use NTP to sync SecureSyncs.

---

**Host Disciplining**

- varies based on type of oscillator installed
- Phase Errors (and TFOMs) can vary widely due to high jitter on the 1PPS being derived from the NTP input

## A) Host Disciplining (NTP input) with a Rubidium oscillator installed

- As of at least v5.8.3 and below (whether the Rb oscillator is using its own internal disciplining, or KTS disciplining in more recent software versions) NTP doesn't discipline Rb oscillators (as I confirmed with Dave S on 8 Jan 2019).

**Email from Dave Lorah** The only way to discipline the oscillator on these Stratum 2 units is to use a 1PPS Input or another stable high quality reference. The NTP simply is not stable enough to discipline the Rubidium.

**Another email from Dave Lorah (20 Dec 16)** I have verified with Engineering support that the Rubidium Oscillator will not discipline if the Securesync is using an NTP Input. This is the same whether you use Timekeeper or not. I am sorry for the confusion.

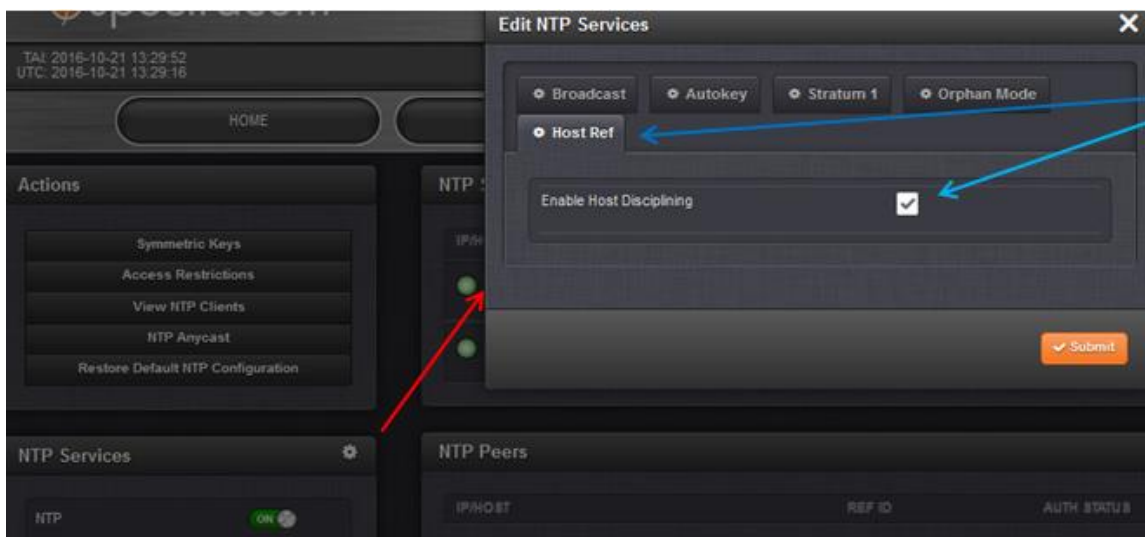
The only way to discipline the oscillator on these Stratum 2 units is to use a 1PPS Input or another stable high quality reference. The NTP simply is not stable enough to discipline the Rubidium.

---

## B) Host Disciplining (NTP input) with an OCXO/TCXO installed

### 1. Versions 5.4.5 and above (Host disciplining is enabled by factory default).

- Software update version 5.4.5 now defaults Host disciplining to OFF by factory default. But a user can enable it in the **Management** -> **NTP Setup** page of the newer browser. Press the gear icon to the right of "NTP Services" and in the pop-up window that opens, select the "Host Ref" tab. Then select the "Enable Host Disciplining" checkbox.
  - **Note:** likely need to also mask the Antenna Problem alarm for the Fault LED to clear.



**(email from Keith, 21 Oct 16)** FYI: Due to some customers preferring the oscillator not be steered by NTP input, update version 5.4.5 added a new checkbox to be able to either enable this function, or to leave it disabled so that NTP doesn't discipline the oscillator.

The factory default setting is this checkbox being disabled (not selected), so that the oscillator is not disciplined by NTP. Since this is a brand new configuration in the software, this checkbox goes to the factory default state after the first update which added it to the software (once selected, updating it again to a newer version of software will return it to the state it was in before updating it). So after updating to version 5.4.5, this checkbox needs to be selected once, if its desired to discipline the oscillator to NTP (thereby clearing the Frequency Error alarm, instead of having to mask this alarm).

The checkbox to enable (or disable it thereafter) NTP host disciplining of the oscillator is in the **Management** -> **NTP Setup** page

of the browser. On the left side of this page, select the gear icon that is just to the right of “NTP Services”. As shown below, select the new “Host Ref” tab, select the “Enable Host Disciplining” checkbox and then press Submit. NTP input will now start disciplining the oscillator again, just like it was before updating the software to version 5.4.5.

### Customer reported TFOMs of around 6 and 7 when syncing via NTP

**Reply from Dave Lorah (22 Sept 15)** This may be the best performance you can hope for using an Internet based NTP Server. The path delays and jitter of the NTP messages depend on the network path and how busy the timer server is. The path delays and jitter are likely just too large with the Internet server to get any better TFOM. If you had a neighboring SecureSync NTP Server located on the same network it would have better performance.

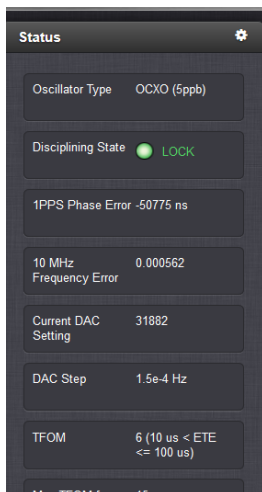
I have setup an SecureSync OXCO system disciplined to an in house close by NTP Server and I am getting TFOM of 6. If you are using an internet time server a TFOM of 7 is not unusual.

**Interesting to note:** I have also been monitoring a system here that is syncing to 66.219.116.140 in Carson City Michigan and it is performing pretty well. It has been running for two hours and TFOM is 5.

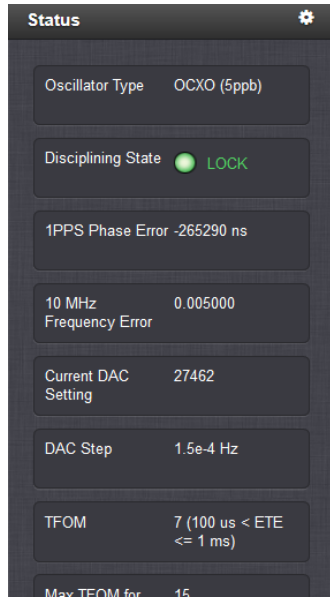
The disciplining should settle in after an hour or two.

### Typical stats we see here when using Host disciplining (OCXO installed)

1. With one of our units (v5.8.3 installed) synced to another unit of ours (**both time servers in the same building**) and with Host Disciplining enabled, we typically see TFOMs of 5 and 6 (phase errors around 50usecs or so) with our time servers (OCXO installed)



2. With our same unit (v5.8.3 installed) used for the test above synced instead to a **NIST INTERNET Time server (129.6.15.28)**, and with Host Disciplining enabled. I am seeing **similar results as above**- TFOMs of 5 to 7 (phase errors around 2-3 usecs to around 300us) with our time servers (OCXO installed) 10 MHz frequency error around 0.000258 Hz to 0.005000 Hz



## 2. Version 5.3.0 (ability to Enable Host disciplining is available – but disabled by factory default)

- version 5.3.0 update added host disciplining for NTP disciplining of TCXO.OCXOs (not Rbs)

## 3. Versions 5.2.1 and below installed (ability to Enable Host disciplining not available).

**Note:** info below with software versions 5.2.1 and below (version 5.3.0 update added host disciplining for NTP disciplining)

- The oscillator is not disciplined with NTP/NTP or User/User modes, when selected as the input reference. In these two modes, the oscillator will remain in free-run mode.
- The System 1PPS is “stepped” as necessary.

When NTP or user set time is the selected reference, the oscillator is not disciplined. It is in free-run mode and the DAC value is not being changed to maintain exactly 10 MHz output. The 1PPS is periodically stepped to align it as necessary. But we are not doing any oscillator disciplining when running with NTP as the synchronizing source.

The Frequency alarm will remain asserted because the oscillator is not being disciplined. But this alarm can be masked in the **Management -> Notifications** page of the web browser (or the **Tools -> Notifications** page of the classic interface browser).

An external 1 PPS reference (other than NTP) should be applied, if it's desired to sync the System Time to NTP and provide accurate 10 MHz output.

Q. From Masataka (“And customer measure phase change of 1PPS from SecureSync by comparing phase difference between 1PPS of SecureSync and 1PPS of sample itself. But as soon as SecureSync sync to stratum1 NTP server (ntp.nict.jp, this phase difference start to expand”).

**A Reply from Keith Wing (6 Jan 15)** Thanks for including the system diagram showing a Stratum 1 server sending NTP time stamps to the SecureSync, as this is important to your customer's observation Your diagram doesn't indicate if the Stratum 1 server is also a SecureSync. But your customer's observations indicate the unit they are likely referring to is

the one labeled "SecureSync" and is getting NTP time from the Stratum 1 server.

To begin, if the SecureSync is syncing to a Stratum 1 NTP time server on the network, NTP in the SecureSync will become Stratum 2 (not Stratum 1). Unless the SecureSync has another higher priority input available (such as GPS or IRIG for examples, or unless it's synced to itself) NTP won't go to Stratum 1 in the SecureSync.

Secondly, the SecureSync's oscillator operation when syncing to NTP is quite different than it is when the SecureSync syncs via other external references such as GPS. When the SecureSync is synced via NTP, the oscillator is not disciplined by the NTP input, as it is when the SecureSync is synced via GPS. Instead, its periodically adjusted, starting after NTP has synced. When the SecureSync syncs via GPS, there is no correlation between the oscillator operation and NTP operation, though shortly after each power-up, both operations are going through process changes at around the same time. Shortly after power-up with GPS available, NTP will be syncing and going to Stratum 1, at around the same time the oscillator is being coarsely adjusted and starting its disciplining. Any observed correlation between NTP going to Stratum 1 and changes to the 10MHz oscillator are strictly coincidental with GPS input, just because of state changes occurring to both operations after every power-up and the SecureSync syncing to GPS.

However, when the SecureSync is being synced via NTP input only (instead of to GPS), the NTP input is influencing the operation of the oscillator, and therefore, also affecting its 10 MHz output. With NTP input synchronization, starting when NTP has synced (gone to one less Stratum than its selected NTP reference- if the reference is Stratum 1, it will go to Stratum 2), the oscillator starts being phase-stepped to bring it into alignment with its NTP input. As long as the SecureSync continues to be synced via NTP, this phase-stepping of the oscillator periodically continues to occur in order to re-align it with its NTP input (because the oscillator is not being continuously disciplined with its 1PPS input). So phase shifts will periodically be observed when syncing via NTP instead of with GPS.

---

### Log entries associated with host disciplining

Note- KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running

**[system] 2015 289 16:31:24 001 HR: Enabling Host Disciplining Mode**

- This entry is asserted each time KHTD is restarted (as indicated in the System log): **KTS Host Time Daemon has restarted (KHTD)**

Note this entry indicates NTP shutdown for halt/reboot by a user (other daemons will also be terminated, as well).

---

### Rubidium oscillator disciplining

#### NOTES:

1. For more info, refer also to the Rubidium oscillator information in the "**SpectraTime SRO-100 Rubidium oscillators**" section in the Customerserviceassistance document
2. Refer to the Oscillator Disciplining documents in the following link for more info:  
[S:\Engineering\Projects\Kramden\KTS\\_Project\\_Development\200\\_Engineering\\_Documents\System\\_Architecture](S:\Engineering\Projects\Kramden\KTS_Project_Development\200_Engineering_Documents\System_Architecture)
3. in at least version 5.8.3 and below, an installed Rb oscillator is not disciplined with NTP/NTP or User/User modes, when selected as the input reference. In these two modes, the oscillator will remain in free-run mode
4. When downgrading from **versions 5.8.0 or above**, to a version **prior to version 5.8.0**, a special patch file needs to be applied.



---

## “XO1” versus “XOS” in oscillator log entries

- How to differentiate between “KTS disciplining” (used with with Rubidium oscillators in versions 5.8.0 and above) versus the Rubidium disciplining itself (used in versions 5.7.x and below)

### A) STANDARD Rubidium disciplining (LPN Rb further below)

#### 1. Software versions 5.8.0 (and above)

- Changed from the Rb disciplining itself, to using the same disciplining as OCXO/TCXO use (KTS disciplining)
  - **(5.8.0 and above) “xos” now annotated in Rb osc log entries:** indicates original disciplining (Rb disciplines itself) in 5.7.x and below
  - Example entry with Rb disciplining itself from v (5.7.x and below)  
**[system] 2018 119 15:56:13 000 XOS: Frequency error recalculated: -00.000005 (-5.194x10<sup>-13</sup>)**

#### 2. Software versions prior to 5.8.0 (5.7.1 and below)

- The Rubidium oscillator internally disciplines itself
  - **(5.7.x and below) “xo1” was being annotated in Rb osc log entries:** indicates Rb is disciplined using KTS (like OCXOs and TCXOs)
  - Example entry with KTS disciplining (5.8.0 and above)  
**[system] 2015 170 07:11:04 000 XO1:**

### B) LPN RB (both RB and OCXO oscillators installed)

#### All software versions

- “XOS” = Rb oscillator disciplining
- “XO1” = OCXO disciplining

**Per email from Dave Sohn (1 July 2020)** XOS messages are valid for LPN Rb units, as we still use the XOS for the RB communication while the XO1 handles the OCXO installed. These are two oscillator systems, so we have two different disciplining elements running.

## C) TCXO/OCXO Disciplining (Disciplining states, D/A DAC values)

### TCXO AND OCXO oscillator disciplining states

- CLI command to read Oscillator Disciplining State: **XO\_GetState 0** <enter>

| New State      | State Value | Meaning                                                                            |
|----------------|-------------|------------------------------------------------------------------------------------|
| Warm-Up        | 1           | At startup/reset. Will stay in this state until a valid time reference is received |
| Calibrate      | 2           | Osc calibration done after startup/reset once a valid reference is found           |
| Tracking Setup | 3           | Quick phase/Qualification.                                                         |
| Tracking Lock  | 4           | Locked into time reference. Constant fine tuning during this state.                |
| Free Run       | 5           | Time reference has been lost. Using oscillator accuracy during holdover.           |

**Note:** There was a State value 6 (“NoRef”) in earlier versions of software. But it was removed in an earlier software update

| Oscillator type          | Refer to section below                                      |
|--------------------------|-------------------------------------------------------------|
| TCXO                     | 1PPS disciplining, when an TCXO oscillator is installed     |
| OCXO                     | 1PPS disciplining, when an OCXO oscillator is installed     |
| Rb                       | 1PPS disciplining, when a Rubidium oscillator is installed. |
| Low phase noise Rubidium |                                                             |

If you have a valid time reference connector to the board, the state should go from “1” to “4”, “4” indicating it has locked in to the reference. If you were to remove the time reference, the state would go to “5” indicating that the unit was now in holdover mode.

When the unit is in state “4” and you were to run the command “XO\_SetMode 0 2”, you should see the state change to “3” indicating that the unit is in the quick phase state and that the tracking has restarted.

Can you verify this on your setup? This will tell us for sure if the “reset tracking” is working in your setup.

---

### TCXO AND OCXO DAC VALUES (D/A VALUES)

Note the **DAC** values in the Oscillator log entries are reported as hex values (“0x”). Convert the hex value to decimal value, via an Internet converter, such as: <https://www.rapidtables.com/convert/number/hex-to-decimal.html?x=D555>

#### A) 1PPS disciplining, when a **TCXO** oscillator is installed

**DAC values:**

- **Min D/A:** 0x0000 (00000 in decimal)
- **Max D/A:** 0xFFFF (65535 in decimal)

**TCXO D/A Vdc steering range:** 0-3 vdc

**Valid D/A range is:** 0x2AAA (10922 in decimal) to 0xD555 (54613 in decimal)

- **“Oscillator Alarm” is asserted** when D/A +/- 10% (0.2vdc) of the valid D/A range

**HR (Hertz range)** is calculated once at the factory and then stored in EEPROM (not erased with a Clean)

Software update version 4.8.6 (June 2012) puts the calibration values in the Oscillator log after every reboot. Refer to the Oscillator log entries in this section for more info.

---

## B) 1PPS disciplining, when an **OCXO** oscillator is installed

### DAC values:

- **Min D/A:** 0x0000
- **Max D/A:** 0xFFFF (**65535** in decimal)

**Valid D/A range is:** 0x2AAA (10922 in decimal) to 0xD555 (54613 in decimal)

**OCXO D/A Vdc steering range:** 0-5vdc

**HR (Hertz range)** is calculated once at the factory and then stored in EEPROM (not erased with a Clean)

Software update version 4.8.6 (June 2012) puts the calibration values in the Oscillator log after every reboot. Refer to the Oscillator log entries in this section for more info.

**“Oscillator Alarm” is asserted** when D/A +/- 10% (0.2vdc) of the valid D/A range ???

### Typical Oscillator log entries with an OCXO installed and being disciplined

Aug 28 19:20:32 Spectracom spectracom: [system] 2012 241 19:20:32 000 New DAC Setting: 0x7F3A (32570 in decimal)  
Aug 28 19:18:52 Spectracom spectracom: [system] 2012 241 19:18:52 000 New DAC Setting: 0x7F3E (32574 in decimal)  
Aug 28 19:18:52 Spectracom spectracom: [system] 2012 241 19:18:52 000 Frequency error recalculated: 00.000050 (5.00<sup>-12</sup>)

Note the **DAC** values in the Oscillator log entries are reported as hex values (“0x”). Convert the hex value to decimal value, via an Internet converter, such as: <https://www.rapidtables.com/convert/number/hex-to-decimal.html?x=D555>

### D/A value not valid

DAC values such as **oxEEEE (61166 decimal)** or **0xD555 (54613 decimal)** indicate a bad OCXO oscillator that needs to be replaced.

**Note:** If the oscillator is failing, the TFOM value may start off, or be drifting, higher than expected (such as TFOM 6 or 7, for example).

If the D/A value appears to have been thrown off, causing problems with oscillator disciplining, (which can affect outputs such as NTP, 10MHz, 1PPS, etc) , there is a **patch.img** file available that can reset the oscillator calibration value back to 0. This causes the board to re-perform the oscillator calibration procedure, with a new cal value calculated and the D/A value being placed at a reasonable value.

---

### Time it takes for OCXO oscillator to lock

- TFOM exceeding MaxTFOM is **10 times faster slew** rate than if MaxTFOM is not exceeded.
  - It only stays at the increased slew rate while MaxTFOM is exceeded. As the System PPS is pulled in, TFOM will continue to decrease. It may eventually fall below MaxTFOM, at which point it slows down to the slower slew rate until its back into alignment.
- Also keep in mind that oscillator disciplining is dependent upon a very stable input PPS. If there is excessive jitter in the reference PPS, oscillator disciplining will be trying to keep up with the jitter. This will inherently help dampen out the input jitter so the System PPS is not as jittery as the reference. But the TFOM may not be able to ever decrease, because it can never actually be able to become aligned with the Reference PPS.

**Email after talking to Mark Goodlein**

After a cold-start, The OCXO oscillators take about 4 minutes to warm-up. A quick-phase oscillator adjustment then occurs as soon as the 1PPS reference has been detected and is considered valid. This quick phase-align adjustment takes about a minute to complete. Then, it takes around 2 minutes for the oscillator to be disciplined "right on".

Total oscillator alignment process time, after a cold start (assuming the input reference is connected at power-up) is about 6 to 7 minutes from power-up.

For the TSync with an OCXO oscillator, the 1PPS is always slewed during re-alignment. The rate at which it is slewed depends upon how the "Maximum TFOM" setting has been configured. This setting allows the user to define how accurate the 1PPS must be in order for the box to report that it is "In Sync".

If the current TFOM value is less than or equal to the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 0.4 Hz (40 ns/s) until the 1PPS is realigned.

If the current TFOM value is more than the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 4 Hz (400 ns/s) until the 1PPS is realigned.

As you can see by these slew rates, it may take a long time to re-align the 1PPS if it is very far off. However, there are always 10 million cycles between each 1PPS (except during power-up).

Keep in mind that it only stays at the increased slew rate while MaxTFOM is exceeded. As the System PPS is pulled in, TFOM will continue to decrease. It may eventually fall below MaxTFOM, at which point it slows down to the slower slew rate until its back into alignment.

80 microseconds of phase error is 80,000 nanoseconds. So if TFOM is not exceeding MaxTFOM, at 40ns/second of slew rate, it will take 2000 seconds (about 30 minutes) for the System PPS to be aligned. However, if TFOM exceeds MAXTFOM, it will speed up to 400ns/second (until TFOM no longer exceeds MaxTFOM, which causes it to slow back down to 40ns/second). Assuming TFOM exceeds MaxTFOM the entire time until it was back into alignment, at 400ns/second, it will take 200 seconds for it to be realigned.

Also keep in mind that oscillator disciplining is dependent upon a very stable input PPS. If there is excessive jitter in the reference PPS, oscillator disciplining will be trying to keep up with the jitter. This will inherently help dampen out the input jitter so the System PPS is not as jittery as the reference. But the TFOM may not be able to ever decrease, because it can never actually be able to become aligned with the Reference PPS. So the TFOM will remain a much higher number than usual.

---

## Using MAX TFOM to go into Holdover Mode/ cause oscillator coarse adjust to occur again

Besides resetting just the timing board itself in order for the oscillator coarse adjustment to automatically occur again (if the TFOM is excessively high), you can also take advantage of the “Max TFOM” value, if you want. If the estimated TFOM value ever exceeds the configured “Max TFOM” value, the coarse adjustment will occur again, until the TFOM value no longer exceeds Max TFOM.

The default Max TFOM is a value of “15”. With Max TFOM still set to the highest possible value of “15”, TFOM is never exceeded. However, you can lower the Max TFOM, so that if estimated timing errors exceed the desired values, the oscillator adjustment will occur much faster, instead of it being slewed very slowly. As the 1PPS is brought in, the TFOM value will decrease., Then, when its much closer, the TFOM will be within its set limits, and it will then switch from coarse adjust to software fine-tune slewing mode.

The Max TFOM value is set using **SS\_setMaxTfom**.

**Example:** The Max TFOM is changed to “5”. If the estimated TFOM is 6 or greater, the TSync will go into Holdover mode and a coarse adjustment occurs, until TFOM becomes 5. Then, it switches back to slewing mode, until TFOM becomes the lower possible value.

---

### A) 1PPS disciplining, when a Rubidium oscillator is installed:

**Note:** For more info, refer also to “Rubidium oscillators” in the “Oscillators/10MHz outputs (for all products)” section in the Custserviceassistance document.

**Notice: the software version installed affects how a Rb oscillator is disciplined**

- **Software versions 5.8.0 and above:** Rb is now disciplined like TCXOs/OCXOs (using KTS firmware)
- Refer to info a little further above: “1PPS disciplining, when an OCXO oscillator is installed”

- **Software versions 5.7.1 and below:** Rb internally disciplines itself to the 1PPS we provide it.

#### **1PPS alignment (both initial alignment and re-alignment after reference is lost/then restored)**

We tell the SRO-100 to use Track mode and then Sync Mode (Track State 1 and then Track State 2) for initial alignment and for re-alignment after a reference is restored.

The SRO-100 first snaps to within 133 ns. Then, it will start to very slowly slew in to the 1PPS input reference. This slewing can takes hundreds of seconds to complete.

#### **Email from Mark Goodlein (11/2/10):**

For the SecureSync with an Rb oscillator, we use a self-disciplining Rb (SpectraTime SRO-100). When the 1PPS reference is restored, our software simply tells the SRO to track it then synchronize to it. The actual behavior is according to the SRO. This is the same behavior as would be found in the Rb NetClock 93XX which uses the same RB oscillator module.

The SecureSync uses the same disciplining algorithm for OCXO as the TSync, which is different from all other products. It has a different way of re-aligning the 1PPS.

#### **Rb oscillator stability after power-up**

- A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.

#### **Email from Dick Fox (6/10/12) to TOYO**

“Our design team is telling me the rubidium needs 2 weeks of GPS disciplining to settle”

**Email from Dick Fox to a customer (6/10/12)**

To obtain predictable drift rates for Rubidium Oscillators you need to:

Keep the units powered. Temperature stability is a major factor in determining the accuracy, so once powered you need to keep them powered.

A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.

SecureSync sets a DAC value that controls the frequency of the Rubidium Oscillator

SecureSync must be synchronized to GPS for a minimum 24 hours before the DAC value is set.

SecureSync will not make any changes to this DAC value unless SS is synchronized to GPS for 24 hours or more.

This means that short GPS syncs will NOT reset the Rubidium frequency and its drift. But short GPS syncs will correct the time offsets.

---

## Oscillator 10 MHz Accuracy (Oscillator accuracy when locked to a reference)

- Oscillator accuracy is based on being locked to an external reference that we can discipline with (such as GPS, IRIG, etc.)
- Our Oscillator accuracy specs (manual and data sheet) are based on GPS being the selected reference

### What if the selected reference is another reference other than GPS (such as IRIG input)?

- Oscillator accuracy will depend on the quality of the external input being provided
- IRIG input
- IRIG DCLS input is better than IRIG AM input
- A SecureSync feeding IRIG DCLS to another SecureSync can achieve synchronization close to that of a 1PPS connection because of how stable the IRIG output of the SecureSync is.

**Email from Dave Sohn (19 Nov 14)** The statement from the manual is a generic statement that we've been looking at revising. The real answer is that the stability and accuracy will depend on the quality of the IRIG provided to the SecureSync. For instance, a SecureSync feeding IRIG DCLS to another SecureSync can achieve synchronization close to that of a 1PPS connection because of how stable the IRIG output of the SecureSync is.

**Email from Dave Sohn (19 Nov 14)** Stability during holdover isn't based at all on the synchronizing reference prior to entry into holdover. It is entirely based on the oscillator and the effects due to aging, temperature, etc. The accuracy will be affected by the input reference. Similar to my email on SecureSync IRIG input, the accuracy of the system will depend on the quality of the IRIG reference.

---

## Effects of NTP peering on the oscillator/System PPS/1PPS outputs

- NTP peering is not recommended for use with Simulcast applications
- No matter what type oscillator is installed (TCXO, OCXO or RB), when NTP peering is used (such as loss of GPS reception for instance), the System 1PPS (and therefore 1PPS outputs also) is dithered to initially align it with the 1PPS obtained from NTP. I believe it's then periodically dithered to keep it aligned to the NTP 1PPS (in at least versions 5.2.1 and below, which don't discipline the oscillator when NTP is the selected reference. Host disciplining is included in update version 5.3.0 - Sept, 2015).
- The moving of the System PPS when peering is active adversely affects simulcast systems that are relying on a stable 1PPS output/
- The only input reference recommended for simulcast is GPS!

---

## \*\*Fractional Frequency Error (FFE) for 10 MHz

- Note: Fractional Frequency errors are reported in "Hertz" (Hz)
- Refer to sites such as: <http://www.nist.gov/pml/div688/generalpubs.cfm>
- Good conversion website: <http://www.convertworld.com/en/frequency/Millihertz.html>

**Notes for using a scientific calculator:**

- Use the “+/- “ and the “Exp” buttons on the calculator to enter values in scientific notation
- The “F-E” button converts the value to scientific notation.

$$\text{FFE} = \frac{\text{Frequency error (which is the measured freq – nominal desired frequency of } 1 \times 10^{+7}\text{)}}{1 \times 10^{+7} \text{ (Nominal desired frequency of “10MHz”)}}$$

Therefore

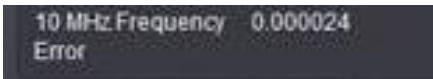
$$\text{FFE for 10MHz} = \frac{\text{Frequency Error (which is the measured freq – } 1 \times 10^{+7}\text{)}}{1 \times 10^{+7}}$$

### Examples

**Email from Tom Richardson (26 Jan 15)** Fractional Frequency error of 1e-11 at 10 MHz is .0001 Hz. Take the error (1e-11) and multiply by the frequency (1e+7) to get the error (1e-4) in Hertz. The error on the screen below is the reverse, take the error in frequency, 0.000024 Hz or 2.4e-5, and divide by the frequency, 10 MHz or 1e7, to get the fractional frequency error, 2.4 e-12.

Given the measured frequency error. Calculate FFE

**First Example:** Measured frequency error in this example is 0.000024 Hz (2.4e-5)



(From **Management -> Disciplining** page of browser)

$$\text{FFE} = \frac{\text{Frequency Error (measured frequency - } 1 \times 10^{+7}\text{)}}{1 \times 10^{+7} \text{ (10 MHz)}}$$

$$\text{FFE} = \frac{0.000024 \text{ Hz (or } 2.4 \times 10^{-5}\text{)}}{1 \times 10^{+7}} = 0.9999999999976 \text{ which is } 2.4 \times 10^{-12} \text{ (negative because } < 1\text{)}$$

**Second Example:** actual measured output frequency is exactly 1 Hz high (10,000,001 Hz)

$$\text{FFE} = \frac{1 \text{ Hz}}{1 \times 10^{+7} \text{ (10MHz)}}$$

So, **FFE** = .0000001 Hz, which is also 1 x 10<sup>-7</sup> Hz (negative because <1)

Given the FFE. Calculate the measured frequency (Hz)



**Note:** use this to calculate expected frequency errors (+/-) based on specs in SecureSync data sheet:

**10 MHz Frequency Output:**

|                                                            | TCXO                | OCXO                | Low Phase Noise OCXO | Rubidium            | Low Phase Noise Rubidium | Fractional Frequency Error (FFE) values |
|------------------------------------------------------------|---------------------|---------------------|----------------------|---------------------|--------------------------|-----------------------------------------|
| <b>Accuracy</b><br>(average over 24 hours when GPS locked) | $1 \times 10^{-11}$ | $2 \times 10^{-12}$ | $1 \times 10^{-12}$  | $1 \times 10^{-12}$ | $1 \times 10^{-12}$      |                                         |

**Example 1 for TCXO:** The TCXO spec for “FFE” from the data sheet is  $1 \times 10^{-11}$  typical

So the known **FFE value** in this case is  $1e^{-11}$

**FFE ( $1e^{-11}$ ) = Frequency error** (which is the measured frequency –  $1 \times 10^7$ )

$1 \times 10^7$  (10 MHz)

**Measured frequency** = multiply ( $1e^{-11}$ ) by  $1 \times 10^7$  = measured frequency of **0.0001 Hz ( $1 \times 10^{-4}$ )**

**To calculate the typical Frequency range** = add to and subtract from 10,000,000 the frequency above.

**Example 2 for OCXO:** The TCXO spec for “FFE” from the data sheet is  $2 \times 10^{-12}$  typical

So the known **FFE value in this case** is  $2e^{-12}$

**FFE ( $2e^{-12}$ ) = Frequency error** (which is the measured frequency –  $1 \times 10^7$ )

$1 \times 10^7$  (10 MHz)

**Measured frequency** = multiply ( $2e^{-12}$ ) by  $1 \times 10^7$  = measured frequency of **0.00002 Hz ( $2 \times 10^{-5}$ )**

**To calculate the typical Frequency range** = add to and subtract from 10,000,000 the frequency above.

## 1200-FAST (Special Frequency Accuracy and Stability test for 10MHz outputs)

- 1200-FAST is a special factory test for 10MHz outputs on the base unit's 10MHz output ports and/or any 10MHz output ports on the option cards as well
- It is to test the Frequency Accuracy and Stability of the 10MHz output(s) of Securesync.
- The price is for per unit (not per output) but you have to tell us what port(s) to test.

Q We have question about the your shipping inspection. Our customer JAXA required us to explain the assurance of 10MHz output accuracy. So, we would like to know how to test 10MHz output and passing conditions.  
We are very glad if your passing condition is like a “when the accuracy of 10MHz output is under  $10^{-12}$ , it passed.”  
We can see your test performance and Test Verification sheet, but it was not written the PASS condition regarding of accuracy.

We do have a specific test for 10MHz outputs Frequency Accuracy and Stability Test, p/n: 1200-FAST.What is a 1200-FAST?

For Securesync (not in the context of JAXA's special applications of 10MHz), the test report typically looks like this:

| Test Verification:  |      |                                                                                         |
|---------------------|------|-----------------------------------------------------------------------------------------|
| Test Point 69       | PASS | $\geq 3.0$ VDC                                                                          |
| Test Point 53       | PASS | $-12.1 \pm 0.6$ VDC                                                                     |
| Test Point 64       | PASS | $5.10 \pm 0.25$ VDC                                                                     |
| Test Point 65       | PASS | $1.240 \pm 0.062$ VDC                                                                   |
| Test Point 66       | PASS | $3.3 \pm 0.2$ VDC                                                                       |
| Test Point 34       | PASS | $3.330 \pm 0.165$ VDC                                                                   |
| Test Point 67       | PASS | $5.00 \pm 0.25$ VDC                                                                     |
| C254                | PASS | $11.00 \pm 0.25$ VDC                                                                    |
| Test Point 54       | PASS | $12.1 \pm 0.3$ VDC                                                                      |
| Program KTS         | PASS | F/W programs successfully without errors                                                |
| J0-J4 10 MHz Output | PASS | 10 MHz @ $2.90 \pm 0.66$ VDC (50 $\Omega$ )                                             |
| Card and SPI BUSS   | PASS | Communicates through BUSS to Installed Option Cards                                     |
| J8 Modem            | PASS | Communicates through NULL Modem                                                         |
| Test Point 52       | PASS | >3 VDC with DC Power only and <500 mVDC with AC power only                              |
| 1PPS Output         | PASS | >4.3 VDCb-p TTL (50 $\Omega$ )                                                          |
| Log Check           | PASS | No System Log errors and No Alarms since Sync                                           |
| GPS Test            | PASS | GPS Power 5 VDC +/- 0.25 VDC, and GPS tracks >4 Satellites w/Q= 3600 (If GPS installed) |

You can see that the 10MHz test points J0 to J4 (which are on the main board) is only rated for amplitude. There is no specific test points for accuracy test as this will require more time to be performed. Also, by check the amplitude, we know the condition of the 10MHz oscillator but bear in mind it is also going to be disciplined by GPS signals as well.

We do have a specific test for 10MHz outputs Frequency Accuracy and Stability Test, p/n: 1200-FAST.

**A Reply from Danny Loke to TOYO (10 April 2019)** 1200-FAST is a special test for 10MHz outputs on the base unit's 10MHz output ports and/or any 10MHz output ports on the option cards as well.  
It is to test the Frequency Accuracy and Stability of the 10MHz output(s) of Securesync.  
The price is for per unit (not per output) but you have to tell us what port(s) to test.

This test is for customer who requires the absolute values of the Frequency Accuracy and Stability measurement of the internal 10MHz oscillator.

**\*Oscillator 10 MHz accuracy (Frequency Error)**

**Frequency Error**

**10 MHz Frequency Output:**

|                                                            | TCXO                | OCXO                | Low Phase Noise OCXO | Rubidium            | Low Phase Noise Rubidium |
|------------------------------------------------------------|---------------------|---------------------|----------------------|---------------------|--------------------------|
| <b>Accuracy</b><br>(average over 24 hours when GPS locked) | 1x10 <sup>-11</sup> | 2x10 <sup>-12</sup> | 1x10 <sup>-12</sup>  | 1x10 <sup>-12</sup> | 1x10 <sup>-12</sup>      |

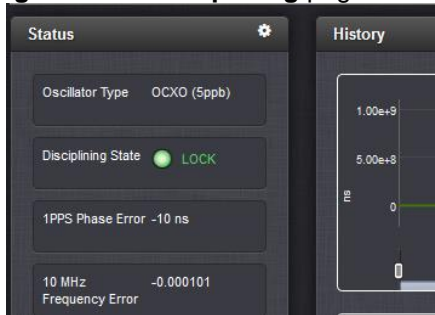
Fractional Frequency Error (FFE)

**Frequency error measurements internal to the SecureSync**

“Raw” Frequency error measurements are reported

**A) Newer web browser (software versions 5.1.2 and above).**

Management -> Disciplining page



**Note:** Typical values for the “raw” frequency errors are like “.000076”

**B) Classic interface browser.**

In the *Status* -> *Disciplining* page

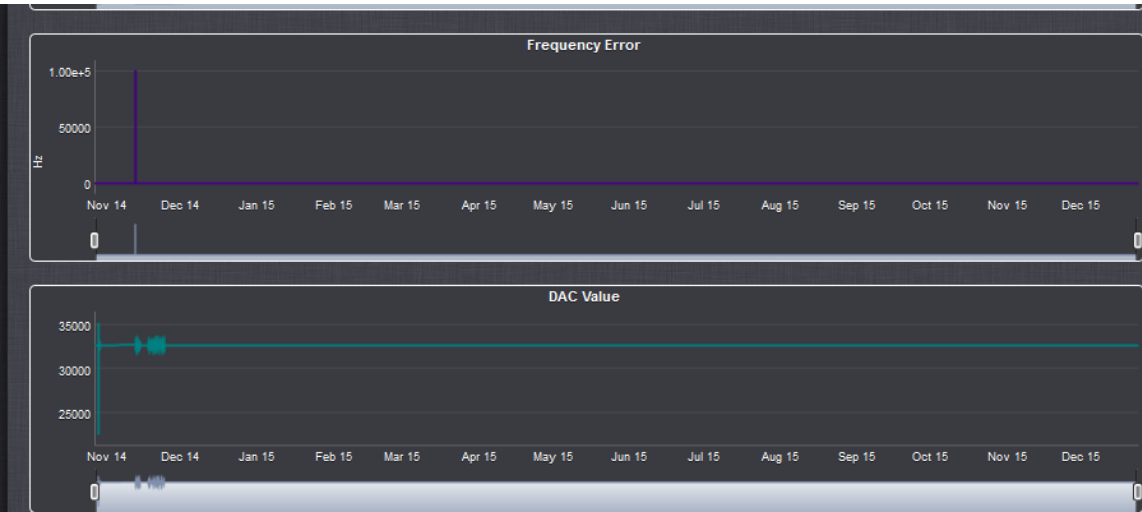
**C) The 10MHz Frequency error can also be read using the `XO_GetFreqError 0` cli command.**

**Monitoring the 10 MHz output (Frequency error and DAC values)**

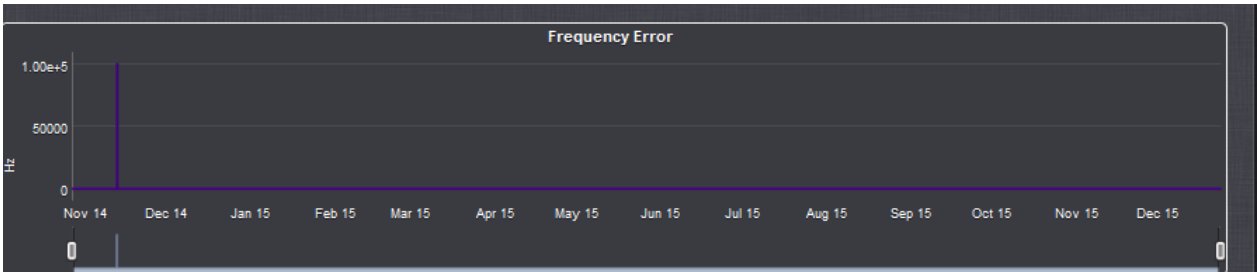
**10 MHz Frequency Error / DAC Value Graphs**

**A) New web browser (versions 5.1.2 and above)**

*Management* -> *Disciplining* page of the browser:



## 1. Frequency Error Graph



### Vertical scale (Hertz)

- Vertical scale is dynamic
- Vertical scale is the “RAW Frequency error” value in Hertz) (its not a Fractional Frequency Error value, like values reported in the Oscillator log)
- Typical values for the “raw” frequency error are like  $1 \times 10^{+/- 4}$ , or  $1 \times 10^{+/- 5}$ , (not like the fractional frequency error values such  $x10^{-11}$ , or  $x10^{-12}$  like we are used to seeing in the Osc log)

### While the oscillator is in free-run

While the oscillator is in Free Run (SecureSync’s in Holdover mode), the Frequency Error will stop being measured and will remain the same value it was last calculated to be, while an external 1PPS reference was still available. The graph will continue to show a straight horizontal line at the same value, until an external 1PPS reference becomes present and valid again.

### Vertical scale

The vertical scale varies depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as  $2e-06$ ).

The scientific breakdown is as follows:

|                            |                           |
|----------------------------|---------------------------|
| <b>1e-12 = 1 pico Hz</b>   | (or 0.000,000,000,001 Hz) |
| <b>1e-11 = 100 nano Hz</b> | (or 0.000,000,000,010 Hz) |
| <b>1e-10 = 10 nano Hz</b>  | (or 0.000,000,000,100 Hz) |
| <b>1e-09 = 1 nano Hz</b>   | (or 0.000,000,001,000 Hz) |
| <b>1e-08= 10 micro Hz</b>  | (or 0.000,000,01 Hz)      |
| <b>1e-07= 0.1 micro Hz</b> | (or 0.0000001 Hz)         |
| <b>1e-06= 1 micro Hz</b>   | (or 0.000001 Hz)          |
| <b>1e-05= 10 micro Hz</b>  | (or 0.00001 Hz)           |
| <b>1e-04= 100 micro Hz</b> | (or 0.0001 Hz)            |
| <b>1e-03= 1 milli Hz</b>   | (or 0.001 Hz)             |
| <b>1e-02= 10 milli Hz</b>  | (or 0.01 Hz)              |
| <b>1e-01= 100 milli Hz</b> | (or 0.1 Hz)               |
| <b>1e+00=1 Hz</b>          | (or 1.0 Hz)               |
| <b>1e+01= 10 Hz</b>        | (or 10.000000000 Hz)      |
| <b>1e+02= 100 Hz</b>       | (or 0100.000000000 Hz)    |
| <b>1e+03= 1000 Hz</b>      | (or 1000.000000000 Hz)    |
| <b>1e+07= 10 MHz</b>       | (or 10,000,000 Hz)        |

**Note:** If the first digit isn't a "1", multiply the first digit by the "time" value in the table above

**Examples:**

- **2e-05= 20 micro Hz** or 0.000020000 ("2" times "10 microseconds" is 20 microseconds)
- **5e-06= 5 micro Hz** or 0.000050000 ("5" times "1 microseconds" is 5 microseconds)

### "Frequency Error recalculated" messages in the Oscillator log

| Id  | Date            | Entity   | Message                                                                              |
|-----|-----------------|----------|--------------------------------------------------------------------------------------|
| 192 | Jan 04 14:11:11 | [system] | 2017 004 14:11:11 000 XO1: Frequency error recalculated: 00.0000397 (3.970x10^-12)   |
| 191 | Jan 04 13:29:31 | [system] | 2017 004 13:29:31 000 XO1: Frequency error recalculated: 00.0000045 (4.547x10^-13)   |
| 190 | Jan 04 12:47:51 | [system] | 2017 004 12:47:51 000 XO1: Frequency error recalculated: -00.0000625 (-6.257x10^-12) |
| 189 | Jan 04 12:06:11 | [system] | 2017 004 12:06:11 000 XO1: Frequency error recalculated: -00.0000559 (-5.592x10^-12) |
| 188 | Jan 04 11:24:31 | [system] | 2017 004 11:24:31 000 XO1: Frequency error recalculated: 00.0000316 (3.166x10^-12)   |
| 187 | Jan 04 10:42:51 | [system] | 2017 004 10:42:51 000 XO1: Frequency error recalculated: -00.0000117 (-1.171x10^-12) |

- If customer is concerned this is an alarm/potential issue, refer customer to the FAQ on our website: <http://support.spectracom.com/articles/FAQ/Why-are-there-so-many-errors-in-the-oscillator-log?q=frequency%20error&>

Q, it also seems to be recalculating frequency error every 40 minutes.

**A Reply from Dave L (5 Jan 17)** The osc Log reports the Frequency Error every 40 minutes. This is not an error but the difference between the oscillator frequency and the GPS Reference frequency. We get questions all the time on this and probably should have used a different word than error in this log. There is nothing wrong. This is normal operation.

When the frequency error measurement exceeds a certain threshold, the Frequency Error Alarm is asserted. The alarm remains until the frequency error drops below the alarm threshold again. This can be caused by a loss of GPS reception, a change in the synchronization reference or even a sudden thermal change.

I can see the unit went into Holdover 1 week four days ago which means it lost GPS for a short time. The internal oscillator would have taken over to provide backup timing until the GPS signal was restored. It appears to be working properly. A loss of GPS from time to time can happen due to heavy weather or mobile GPS jammers.

I do not think this unit is malfunctioning. I do recommend updating the firmware though. Version 5.1.5 is a few years old. We

currently have version 5.5.1 on our website. Please consider updating at your convenience.

Here is a link to the firmware on our website: <https://spectracom.citrixdata.com/share?#/view/sb15ef818d73417e9>

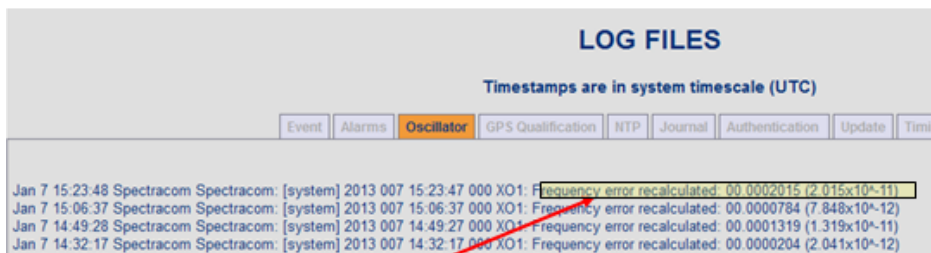
**Typical values for a good OCXO, when locked to GPS: no worse than around “ 5.994x10<sup>-11</sup>”**

**Email from Dave Sohn (28 Jan 2015)** With a typical reference, I believe that the minimum non-zero value we can report is +/- 6.25e-13.

Spectracom SecureSyncs contain one of five types of internal 10 MHz oscillators. The internal oscillator is used to output 10 MHz and to generate an internal 1PPS signal.

The “Oscillator” log provides an indication of the frequency counts of the oscillator’s 10 MHz output, as measured using the selected 1PPS Input Reference (Such as a GPS receiver’s 1PPS output signal) as a reference.

The “frequency error recalculated” messages in this log indicate the accuracy of the oscillator output, in comparison to a perfect 10 MHz signal (known as the “fractional frequency error”). The 10 MHz oscillator output is measured against the 1PPS generated by the selected 1PPS input reference.



The phrase “FREQUENCY ERROR RECALCULATED” designates the value to follow is reporting how close the oscillator’s actual 10 MHz output signal is to the desired frequency of 10.0000000 MHz (reported in scientific notation). This phrase is not an indication that there is a problem with the oscillator.

**Important Note-** The “FREQUENCY ERROR RECALCULATED” phrases displayed on this web page DO NOT mean a problem exists with either the internal oscillator or with the NTP server. “FREQUENCY ERROR RECALCULATED” refers to the Fractional Frequency Error which is a comparison of the actual output frequency versus the desired frequency (The desired frequency is 10.0000000 MHz), reported in scientific notation. This phrase will ALWAYS be present on this page to show the measured 10 MHz frequency. If a problem DOES happen to exist with the oscillator frequency measurements, a Frequency alarm will be entered in the “Alarms” log.

The lower the “Frequency error recalculated” value is, the closer the oscillator is to outputting an exact 10 MHz signal. Below is a table of the 10MHz specifications. The “Frequency error calculated” values should typically be less than the values in the “Short term Stability” section of this table, for the specific type of oscillator installed, as long as SecureSync is synced to an external reference (other than other NTP servers).

### 10 MHz Frequency Output:

|                                                                         | TCXO                    | OCXO                     | Low Phase Noise OCXO     | Rubidium                                                           | Low Phase Noise Rubidium                                           |
|-------------------------------------------------------------------------|-------------------------|--------------------------|--------------------------|--------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>Accuracy</b><br>(average over 24 hours when GPS locked)              | 1x10 <sup>-11</sup>     | 2x10 <sup>-12</sup>      | 1x10 <sup>-12</sup>      | 1x10 <sup>-12</sup>                                                | 1x10 <sup>-12</sup>                                                |
| <b>Medium Term Stability</b><br>(without GPS after 2 weeks of GPS lock) | 1x10 <sup>-8</sup> /day | 5x10 <sup>-10</sup> /day | 2x10 <sup>-10</sup> /day | 5x10 <sup>-11</sup> /month<br>(3x10 <sup>-11</sup> /month typical) | 5x10 <sup>-11</sup> /month<br>(3x10 <sup>-11</sup> /month typical) |
| <b>Short Term Stability (Allan variance)</b>                            |                         |                          |                          |                                                                    |                                                                    |
| 1 SEC                                                                   | 2x10 <sup>9</sup>       | 5x10 <sup>-10</sup>      | 5x10 <sup>-11</sup>      | 2x10 <sup>-11</sup>                                                | 5x10 <sup>-10</sup>                                                |
| 10 SEC                                                                  | 1x10 <sup>9</sup>       | 5x10 <sup>-11</sup>      | 2x10 <sup>-11</sup>      | 2x10 <sup>-12</sup>                                                | 2x10 <sup>-11</sup>                                                |
| 100 SEC                                                                 | 3x10 <sup>-10</sup>     | 1x10 <sup>-11</sup>      | 1x10 <sup>-11</sup>      | 2x10 <sup>-12</sup>                                                | 5x10 <sup>-12</sup>                                                |

**“Frequency error recalculated: 00.000000 (0.000x10<sup>-16</sup>)” (0.000e-16 or 0.000x10-16)**

**Note:** This oscillator.log entry can be asserted for one of two reasons:

#### **A) The actual frequency error is less than we can measure**

**Email from Dave Sohn (27 Jan 15)** after I alluded to the software issue below It is still possible to receive a frequency error of 0 if it is below our measurement capability. We fixed where negative frequency errors were reported as 0.

**Edited Email Keith sent to Masataka (27 Jan 15)** Thanks for forwarding along your customer’s inquiry about the oscillator log entries.

The oscillator log entry of **“Frequency error recalculated: 00.000000 (0.000x10<sup>-16</sup>)”** is not a symptom of any problems occurring with the SecureSync. These log entries just mean that the magnitude of the frequency error at that time was less than the threshold that the system can even measure. In this case, the Frequency Error is reported as “0.000x10<sup>-16</sup>” (the lowest value possible for the system to report). So instead of these log entries being a symptom of a problem, they instead indicate the oscillator is as close to being at the desired frequency as the system is capable of measuring.

**Email from Dave Sohn (28 Jan 2015)** With a typical reference, I believe that the minimum non-zero value we can report is +/- 6.25e-13.

#### **B) A minor software issue in software versions 5.10 through 5.1.4 (fixed in 5.1.5)**

- Software issue with reporting the frequency error in the Oscillator log
- Negative values were being incorrectly being reported as “0” (“So any negative frequency error measurements will show as 0.000x10-16.”)
- Refer to Mantis case 2862 <http://cvsmantis.int.rolia.com/mantis/view.php?id=2862>
- This issue first started in version 5.1.0.
- Fixed in version 5.1.5 software update

**Email from Dave Lorah to Masataka (24 June 2014)** The minimum measurable values are based on the error range of the reference, the adjustable measurement window, and the oscillator type, but it should be in the range 10x-13.

I was incorrect saying the 0.000x10-16 was reporting a 0 value, actually the 10x-16 is no measurable error. I found out there is a bug in the current logging that reports negative values as 10x-16. They are displayed correctly in the disciplining pages in the UI, but the log entries will have the issues. So any negative frequency error measurements will show as 0.000x10-16.

As far as changes between 5.0.2 and 5.1.4, we improved our measurement window adjustments, improved our initial sync time performance, and added adjustable filtering based on input reference error. There would be a difference in the oscillator

log measurements due to these changes. The oscillator measurement range should be in the x10-11 to x10-13 range. The oscillator log you sent us shows typical performance.

Software version 5.1.4 improvements to oscillator disciplining

**Email from Dave Lorah to Masataka (24 June 2014)** As far as changes between 5.0.2 and 5.1.4, we improved our measurement window adjustments, improved our initial sync time performance, and added adjustable filtering based on input reference error. There would be a difference in the oscillator log measurements due to these changes. The oscillator measurement range should be in the x10-11 to x10-13 range. The oscillator log you sent us shows typical performance.

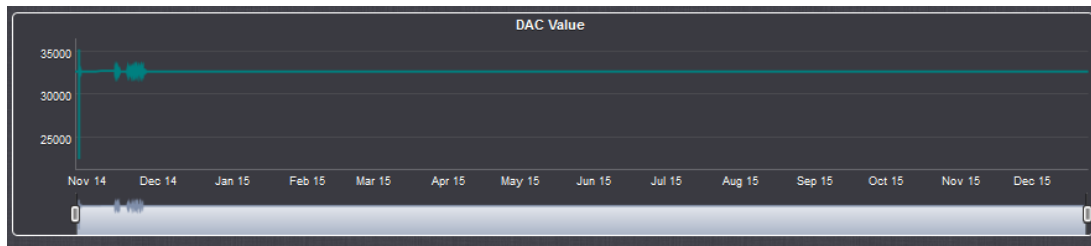
---

## “Rb Reference unstable” / “Rb synchronized” / “Rb track off -- free run”

- Could indicate a bad Rb oscillator
- Can also be caused by issues with the selected 1PPS reference (such as issues with a Res-SMT-GG receiver)
  - The “Rb Reference unstable” alarm was seen correlated with the following entry in the Timing log  
“[system] 2014 291 13:01:08 002 Error: CS\_Set(CS\_SA\_LEAP\_SEC) call from GR.”
  - The “Rb Reference unstable” alarm was seen correlated with the following entries in the oscillator log  
[system] 2016 048 17:02:00 000 XOS: Rb Reference unstable  
[system] 2016 048 17:02:01 000 XOS: Rb tracking  
system] 2016 048 17:02:32 000 XOS: Rb synchronized  
[system] 2016 048 17:03:08 000 XO1: Phase Err: -31170.0  
[system] 2016 048 17:03:08 000 XO1: Freq Err: +0.132500

---

## DAC Value Graph



---

## Frequency Error measurements, while the oscillator is in free-run

While the oscillator is in Free Run (SecureSync's in Holdover mode), the Frequency Error **will stop being able to be calculated**. So the DAC value will remain at its last calculated value, while the oscillator remains in free-run (no changes are made to the DAC value while in Holdover mode).

---

## To download the raw oscillator data (not applicable to the classic interface browser)

- A “.csv” or “.json” file with the oscillator values (and system temperatures) can be downloaded as desired.

Download of raw oscillator data as a “.csv” file (can be opened in excel)

**A “.csv” file can be downloaded using either of two different methods:**

1. **A .CSV file download button is available in the Management -> Disciplining page of the browser**

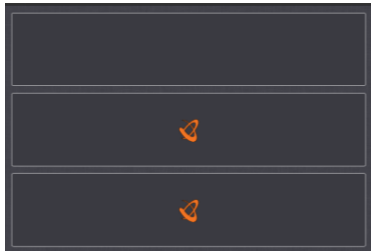
From the **Management -> Disciplining** page of the browser (click on the “down arrow” ICON on the right side of the page to download the .csv file. Press the garbage can icon to delete all of the oscillator and temperature data used to display the graphs)





**Note:** The “garbage can” ICON on the upper-right corner clears/deletes all of the graph data.

**Note:** Deleting the log data will refresh the graphs.



## 2. Manually enter the link to the OscillatorStatuslog.csv

If you manually enter `/logs/OscillatorStatusLog.csv` after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

**Example:** <http://10.10.128.1/logs/OscillatorStatusLog.csv> (change address as applicable)

**Example .csv file output below (“Sys temp” and “CPU temp” fields were added in software version 5.3.0)**

| id    | sys_timestamp    | sync | holdover | time_ref | pps_ref | dac   | phase_error | freq_error | sys_temp | cpu_temp | disc_temp |
|-------|------------------|------|----------|----------|---------|-------|-------------|------------|----------|----------|-----------|
| 63102 | 11/18/2015 15:45 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63101 | 11/18/2015 15:43 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63100 | 11/18/2015 15:42 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63099 | 11/18/2015 15:41 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63098 | 11/18/2015 15:40 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63097 | 11/18/2015 15:39 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 99       | 0         |
| 63096 | 11/18/2015 15:38 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63095 | 11/18/2015 15:36 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63094 | 11/18/2015 15:34 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63093 | 11/18/2015 15:33 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63092 | 11/18/2015 15:32 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 99       | 0         |
| 63091 | 11/18/2015 15:31 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 80       | 100      | 0         |
| 63090 | 11/18/2015 15:30 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63089 | 11/18/2015 15:29 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 98       | 0         |

### Definition of fields

**Sync and Holdover:** 1 is true, 0 is false

**Time ref and PPS ref:** Selected input reference at that time

**DAC:** Oscillator’s DAC value

**Phase Error:** 1PPS Phase Error

**Freq Error:** Oscillator’s Fractional Frequency Error

|   | freq_error  | is |
|---|-------------|----|
| 3 | -0.00064398 |    |
| 2 | -0.00064398 |    |
| 3 | -0.00064398 |    |
| 3 | 6.85E-05    |    |
| 3 | 6.85E-05    |    |
| 5 | 6.85E-05    |    |
| 1 | 6.85E-05    |    |
| 1 | 6.85E-05    |    |
| 3 | 6.85E-05    |    |
| 3 | 6.85E-05    |    |
| 5 | 6.85E-05    |    |
| 1 | 6.85E-05    |    |
| 1 | 0.000250182 |    |
| 1 | 0.000250182 |    |
| 1 | 0.000250182 |    |
| 2 | 0.000250182 |    |
| 7 | 0.000250182 |    |
| 3 | 0.000250182 |    |
| 3 | 0.000250182 |    |
| 3 | 0.000250182 |    |
| 7 | 0.000250182 |    |

## Temps: Board, CPU and Oscillator

### Notes:

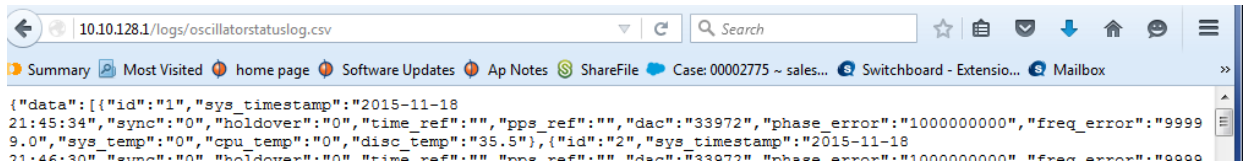
1. **Oscillator** temp is only available if the temperature sensor (U60) is installed on the main PCB (very close to the oscillator). Refer to ECN 2807 (5 Dec,2011)
2. **Board** and **CPU** temps were added in software version 5.3.0

## C) Output of graphable oscillator and temperature data as a .json file for graphing

Same process as downloading.csv file with direct link, but replace “.csv” with “.json” instead.

If you manually enter **/logs/OscillatorStatusLog.json** after the URL of the SecureSync in the web browser it will download a json file.

**Example:** <http://10.10.128.1/logs/OscillatorStatusLog.json> (change address as applicable)



## Frequency Error measurements while in oscillator Free-Run mode (SecureSync in Holdover mode)

- While the oscillator is in in Free Run, the Frequency error stops being calculated and remains at the last calculated value. To determine if the frequency error is the current or the last calculated value, user needs to determine if the oscillator is locked or currently in free run.
- Because the frequency error measurements stop being calculated while the oscillator is in free run mode, an external frequency counter (such as the Spectracom frequency counters, Models CNT-90 or CNT-91) should be used to measure the Frequency Error while SecureSync is in Holdover mode (oscillator free run).

## Typical/expected Frequency Error calculations when not locked

Below are the typical expected measurements of the 10MHz output. Note these are not specs, but averages over a period of 24 hours.

10 MHz Frequency Output:

|                                                                                        | TCXO                   | OCXO                    | Low Phase Noise OCXO    | Rubidium                                                         | Low Phase Noise Rubidium                                         |
|----------------------------------------------------------------------------------------|------------------------|-------------------------|-------------------------|------------------------------------------------------------------|------------------------------------------------------------------|
| <b>Medium Term Stability</b><br><small>(without GPS after 2 weeks of GPS lock)</small> | 1x10 <sup>9</sup> /day | 5x10 <sup>10</sup> /day | 2x10 <sup>10</sup> /day | 5x10 <sup>11</sup> /month<br>(3x10 <sup>11</sup> /month typical) | 5x10 <sup>11</sup> /month<br>(3x10 <sup>11</sup> /month typical) |
| <b>Short Term Stability (Allan variance)</b>                                           |                        |                         |                         |                                                                  |                                                                  |
| 1 SEC                                                                                  | 2x10 <sup>9</sup>      | 5x10 <sup>10</sup>      | 5x10 <sup>11</sup>      | 2x10 <sup>11</sup>                                               | 5x10 <sup>10</sup>                                               |
| 10 SEC                                                                                 | 1x10 <sup>9</sup>      | 5x10 <sup>11</sup>      | 2x10 <sup>11</sup>      | 2x10 <sup>12</sup>                                               | 2x10 <sup>11</sup>                                               |
| 100 SEC                                                                                | 3x10 <sup>10</sup>     | 1x10 <sup>11</sup>      | 1x10 <sup>11</sup>      | 2x10 <sup>12</sup>                                               | 5x10 <sup>12</sup>                                               |
| <b>Temperature Stability</b><br><small>(back to back)</small>                          | 1x10 <sup>6</sup>      | 5x10 <sup>9</sup>       | 1x10 <sup>9</sup>       | 1x10 <sup>10</sup>                                               | 1x10 <sup>10</sup>                                               |

Fractional Frequency Error (FFE)

### TCXO/OCXO frequency error

- Measurements with a TCXO/OCXO can be either positive or negative numbers.

### Rubidium oscillator frequency errors

- Frequency Error observed on our House reference (10.10.10.2 with Low phase noise rb): -000026ns
- Measurements with a Rb oscillator will always be reported as a positive number, even if it's a negative value

Per Dave Sohn (15 May 2014) Keith, I also believe the Rb error calculation is always provided as a magnitude value error, which means that regardless of whether it is actually positive or negative it is returned as a positive value.

Q. About phase error/frequency error. We would like to know physical meaning of these numbers so we can properly interpret and try to use them in our measurement analysis

A. Frequency and phase error for the Rubidium are both provided as unsigned magnitude values. Frequency error is determined by the phase error accumulated during a period of time equal to the tracking loop constant as determined by the Rubidium disciplining. The tracking loop constant starts at 1000s, but can grow and shrink depending on quality of the reference and other conditions. The phase error is determined from the current phase error comparator value plus the measured error fluctuation of the reference.

Q. Is temperature stability data available for SecureSync? The only data we have is p-p frequency error across operating temperature range from specification. We have found that the phase error anomaly is very likely rack temperature related and it would be helpful to know tolerance limits and optimal working temperature.

A Per Dave Sohn (22 May 2014) We specify the temperature stability across the entire range as provided from our oscillator vendor. We do not have information on optimal or more problematic temperature ranges.

### Freq error of 0.00e+00

Per Dave Sohn (15 May 2014) Seeing a zero value for the frequency error is not an indicator of any issues. It just means that the error is less than what we can measure for that period.

### Oscillator Accuracies (From the SecureSync Data Sheet):

**Important Note:** these average accuracy specs below are average over 24 hours when locked to GPS.

### 10 MHz Frequency Output:

|                                                            | TCXO                | OCXO                | Low Phase Noise OCXO | Rubidium            | Low Phase Noise Rubidium |
|------------------------------------------------------------|---------------------|---------------------|----------------------|---------------------|--------------------------|
| <b>Accuracy</b><br>(average over 24 hours when GPS locked) | $1 \times 10^{-11}$ | $2 \times 10^{-12}$ | $1 \times 10^{-12}$  | $1 \times 10^{-12}$ | $1 \times 10^{-12}$      |

**TCXO:**  $1 \times 10^{-11}$  Hz/day=

$1 \times 10^{-11}$  Hz/day = 0.00000000001 Hz/ day = 0.01 nano Hz/day

**OCXO**  $2 \times 10^{-12}$  Hz/day=

$2 \times 10^{-12}$  Hz/day = 0.000000000002 Hz /day = 0.002 nano Hz /day

**Low Phase Noise OCXO**  $1 \times 10^{-12}$

$1 \times 10^{-12}$  Hz/day= 0.000000000001Hz/day = 0.001 nano Hz /day

**Low Phase Noise Rb**  $1 \times 10^{-12}$

$1 \times 10^{-12}$  Hz/day= Hz/day= 0.000000000001 Hz/day = 0.001 nano Hz /day

## Holdover mode/ Oscillator 10 MHz free-run (Oscillator Stability)

### Oscillator stability

#### Several factors affect oscillator stability

- Aging rate
- Temperature variations
- Oscillator's input Power fluctuations
- Humidity variations
- And others

Oscillator drift is essentially the oscillator aging rate, plus temperature drift, plus the effects of other variables.

#### Factors that don't affect stability:

- The Selected reference before oscillator goes into Free run mode (such as IRIG input instead of GPS)

**Email from Dave Sohn (19 Nov 14)** The statement from the manual is a generic statement that we've been looking at revising. The real answer is that the stability and accuracy will depend on the quality of the IRIG provided to the SecureSync. For instance, a SecureSync feeding IRIG DCLS to another SecureSync can achieve synchronization close to that of a 1PPS connection because of how stable the IRIG output of the SecureSync is.

**Email from Dave Sohn (19 Nov 14)** Stability during holdover isn't based at all on the synchronizing reference prior to entry into holdover. It is entirely based on the oscillator and the effects due to aging, temperature, etc. The accuracy will be affected by the input reference. Similar to my email on SecureSync IRIG input, the accuracy of the system will depend on the quality of the IRIG reference.

**Important note:** Drift is non-linear

**Email from Dave Sohn (17 Oct 2013)** Drift in holdover is not linear as implied here. The phase drift will be exponential as the frequency drifts. So, no oscillator will provide <1ms per day indefinitely. For example, the TSync OCXO will provide less than 1ms per day for around 6-7 days, but more than that afterwards. Also, all of our models are based on good starting values starting out from GPS synchronization, which won't be available here.

**Email from Tony Diflorio to a potential customer looking for 1ms/day accuracies** A couple of other ideas to help you: You could use a portable (battery operated) GPS synchronization device to provide re-synchronization to the TSync-PCIe-Opt-OCXO card, such as our model GPS-12/12R (see attached). This re-synchronization would have to be done every few days though to maintain the TSync-PCIe-OCXO to <1ms per day of drift. Or, you might be able to use our popular “SecureSync”, rack mounted GPS Synchronization system (see attached) with a Rubidium internal oscillator. This depends on whether you must have specific features that only a Bus-Level card can provide. Using our SecureSync with a Rubidium internal oscillator will provide the holdover accuracy you are looking for, over a much longer period of time (almost indefinitely).

**Oscillator stability with reference removed (in freeun)**

**1PPS output holdover specs with OCXO oscillator**

**Email from Dave Sohn (10/3/11)** regarding low phase noise drift (no GPS) after at least two weeks of lock: Estimate for holdover at constant temperature after 2 weeks of GPS lock

| Days | Drift  |
|------|--------|
| 1    | 10 us  |
| 2    | 40 us  |
| 3    | 80 us  |
| 7    | 430 us |

**Email from Tim Tetreault to Will Hickey:**

Will,  
The Holdover spec's for the TCXO is the same between the TSync and SecureSync:

Standard TCXO:  
450usec/24hr (constant temp after 2 weeks of GPS lock)

The Holdover spec's for the OCXO is not the same because they use different OCXO's. The spec for the TSync is:

Optional OCXO:  
90usec/24hr (constant temp after 2 weeks of GPS lock)

So if the customer wanted to calculate the drift per seconds:  
The TCXO would be:  
 $45E-5 / (60sec \times 60min \times 24 \text{ hours}) = 5.2 \text{ ppb}$

The error for the OCXO would be:  
 $9E-5 / (60sec \times 60min \times 24 \text{ hours}) = 1.0 \text{ ppb}$

- **Disciplined to Timecode:**  $2 \times 10^{-7}$
- **Undisciplined Freewheel Drift:**  $1 \times 10^{-6}$

**Oscillator stability when the board is in holdover mode:**

- TCXO our oscillator stability is  $1E-6$  (1 ppm),
- OCXO our oscillator stability is  $5E-8$  (50 ppb).

There are two main error factors for oscillator stability – Initial startup and aging over time. The initial startup and lifetime aging specs are as follows:

| Oscillator      | Initial startup | Lifetime aging |
|-----------------|-----------------|----------------|
| OCXO oscillator | 0.2 PPM         | 2.0 PPM        |
| TCXO oscillator | 1.0 PPM         | 5.0 PPM        |

With an external input reference (such as GPS and IRIG), we can account for these errors.

### A) To calculate the estimated amount of Freewheel drift with a TCXO:

Convert the time to seconds and multiply by 1.5E-6.

Examples (where 1 hr = 3600sec):

**Amount of drift per hour** =  $3600 * 1.5E-6 = 0.0054$  seconds per hour (or **5.4 milliseconds**) of estimated drift

**Amount of drift per second**=  $0.0054\text{sec} / 3600$  (seconds) =  $.0000001$  seconds per second (or **0.1 microseconds**) of estimated drift

**Amount of drift per day**=  $0.0054\text{sec} * 24$  (hours) =  $.123$  seconds per day (or **12 milliseconds**) of estimated drift

### B) To calculate the estimated amount of Freewheel drift with an OCXO:

Convert the time to seconds and multiply by 5E-8.

Examples (where 1 hr = 3600sec):

**Amount of drift per hour** =  $3600 * 5E-8 = 0.00018$  seconds per hour (or **0.18 milliseconds**) of estimated drift

**Amount of drift per second**=  $0.00018\text{sec} / 3600$  (seconds) =  $0.00000005$  seconds per second (or **0.05 microseconds**) of estimated drift

**Amount of drift per day**=  $0.00018 \text{ sec} * 24$  (hours) =  $0.00432$  seconds per day (or **4.32 milliseconds**) of estimated drift

---

### Selected reference (GPS, IRIG, etc) before Holdover/oscillator free run begins

Q What type of input reference (GPS, IRIG, external PPS, etc) that was selected before the oscillator goes into Freerun mode has no effects on free-run operation.

**A Dave Sohn (19 Nov 2014)** Stability during holdover isn't based at all on the synchronizing reference prior to entry into holdover. It is entirely based on the oscillator and the effects due to aging, temperature, etc. The accuracy will be affected by the input reference. Similar to my email on SecureSync IRIG input, the accuracy of the system will depend on the quality of the IRIG reference.

---

### Oscillator aging rates

- Refer to: [:\Engineering\Oscillators](#)
- Aging rates are based on 30 days of continuous operation
- Rates are much higher with less than 30 days of operation (it's a huge curve)

#### Examples:

**SRO-100 Rb oscillator:** Aging rate is  $< 5E-11$ /month (after 30 days of continuous operation)

## Our Specs

- Medium term Stability is over a longer period of time (such as either after 24 hours or after 1 month, as specified)
- Short term Stability is over short “windows” of time (such as in just 1 second, over 10 seconds, or over 100 seconds).
- Our specs (discussed below) are TYPICAL or average values – not Absolute values!

### Oscillator Medium Term stability in free run: From SecureSync Data Sheet (with some modification for presentation)

- “Holdover” values over one day or one month (as specified)

**Important Note:** this medium term stability specs below are average values upon loss of input reference that has been present for at least two weeks (system running the whole time). Shortening this period can severely degrade these values.

#### 10 MHz Frequency Output:

|                                                                         | TCXO                    | OCXO                     | Low Phase Noise OCXO     | Rubidium                                                            | Low Phase Noise Rubidium                                            |
|-------------------------------------------------------------------------|-------------------------|--------------------------|--------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Medium Term Stability</b><br>(without GPS after 2 weeks of GPS lock) | $1 \times 10^{-8}$ /day | $5 \times 10^{-10}$ /day | $2 \times 10^{-10}$ /day | $5 \times 10^{-11}$ /month<br>( $3 \times 10^{-11}$ /month typical) | $5 \times 10^{-11}$ /month<br>( $3 \times 10^{-11}$ /month typical) |

**TCXO:**  $1 \times 10^{-8}$  per day

- $1 \times 10^{-8}$  Hz/day = 0.00000001 Hz/day = 10 nano Hz/day

**OCXO**  $5 \times 10^{-10}$  per day

- $5 \times 10^{-10}$  Hz/day = 0.0000000005 Hz/day = 0.5 nano /day

**Low Phase Noise OCXO**  $2 \times 10^{-10}$  per day

- $2 \times 10^{-10}$  Hz/day = 0.0000000002 Hz/day = 0.2 nano Hz /day

**Rubidium**  $5 \times 10^{-11}$  per month

- $5 \times 10^{-11}$  Hz/month = 0.00000000005 Hz/month = 0.05 nano Hz /month
- $3 \times 10^{-11}$  Hz/month typical = 0.00000000003 Hz/month = 0.03 nano Hz /month

**Low Phase Noise Rb**  $5 \times 10^{-11}$  per month

- $5 \times 10^{-11}$  Hz/month = 0.00000000005 Hz/month = 0.05 nano Hz /month
- $3 \times 10^{-11}$  Hz/month typical = 0.00000000003 Hz/month = 0.03 nano Hz /month

### Oscillator Short Term stability in free run: From SecureSync Data Sheet (with some modification for

**presentation)**

- “Holdover” values over very short “windows of time (such as 1 second to the next, over just 10 seconds, or over just 100 seconds)

**10 MHz Frequency Output:**

|                                                | TCXO                | OCXO                | Low Phase Noise OCXO | Rubidium            | Low Phase Noise Rubidium |
|------------------------------------------------|---------------------|---------------------|----------------------|---------------------|--------------------------|
| <b>Short Term Stability (Allan variance)</b>   |                     |                     |                      |                     |                          |
| 1 Sec                                          | $2 \times 10^{-9}$  | $5 \times 10^{-10}$ | $5 \times 10^{-11}$  | $2 \times 10^{-11}$ | $5 \times 10^{-11}$      |
| 10 Sec                                         | $1 \times 10^{-9}$  | $5 \times 10^{-11}$ | $2 \times 10^{-11}$  | $2 \times 10^{-12}$ | $2 \times 10^{-11}$      |
| 100 Sec                                        | $3 \times 10^{-10}$ | $1 \times 10^{-11}$ | $1 \times 10^{-11}$  | $2 \times 10^{-12}$ | $5 \times 10^{-12}$      |
| <b>Temperature Stability</b><br>(peak-to-peak) | $1 \times 10^{-6}$  | $5 \times 10^{-9}$  | $1 \times 10^{-9}$   | $1 \times 10^{-10}$ | $1 \times 10^{-10}$      |

**Oscillator D/A value while in Holdover/reboot (TCXO/OCXO)**

The following info is for TCXO and OCXO oscillators. If they have a Rb oscillator, let me know and I will check with our Engineering team to see if it’s similar to these other two oscillators.

When the SecureSync goes into Holdover mode (loses all input references), the D/A remains the same value it was before the reference(s) was lost. Because disciplining stops when there are no references, this D/A will remain constant thereafter, until at least one input reference is restored and declared valid

The D/A value is stored, so after a reboot/power cycle, the D/A value is restored to the same value it was before the reboot.

**Low phase noise (HP) oscillator free run**

**Email from David Sohn to Dick Fox.**

The holdover for one day would be around 10 microseconds, but the drift is not linear, it’s exponential. Based on our model, the drift after 14 days would be around 1.7 milliseconds.

**Email from Dick to TOYO (based on input from Dave Sohn)**

**To obtain predictable drift rates for Rubidium Oscillators you need to:**

- keep the units powered. Temperature stability is a major factor in determining the accuracy so once powered you need to keep them powered
- A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.
- Secure Sync sets a DAC value that controls the frequency of the Rubidium Oscillator
- Secure Sync must be synchronized to GPS for a minimum 24 hours before the DAC value is set.
- Secure Sync will not make any changes to this DAC value unless SS is synchronized to GPS for 24 hours or more
- This mean that short GPS syncs will NOT reset the Rubidium frequency and its drift



- But short GPS syncs will correct the time offsets

Based on this, Spectracom can commit to a drift rate of 5 X10<sup>-12</sup> per month provided

- The units is initially synchronized to GPS for a minimum of 2 weeks
- The unit isn't powered off after it was synchronized

If this is acceptable?

Here is what the drift rate table looks like

- The 2 hours of GPS lock – initializes Secure Sync's 1 PPS to track UTC within +or-25 nanosecond standard deviation
- No adjustment to the oscillator frequency is made
- The 4 hours of GPS lock – initializes Secure Sync's 1 PPS to track UTC within +or-25 nanosecond standard deviation
- No adjustment to the oscillator frequency is made
- The 24 hours of GPS lock – initializes Secure Sync's 1 PPS to track UTC within +or-25 nanosecond standard deviation
- The DAC value that controls the Rubidium oscillator frequency can be adjusted

There is little incremental value is syncing to GPS for 4 hours versus 2 hours. It doesn't adjust the Rubidium oscillator frequency just correct the time.

Only GPS lock for 24 hours or more adjusts the oscillator frequency.

Here is the table

| GPS lock time                | 2 hours  | 4 hours   | 24 hours |
|------------------------------|----------|-----------|----------|
| > After 4 hours of holdover  | .20 usec | 0.20 usec | 0.2 usec |
| > After 24 hours of holdover | 2 usec   | 2 usec    | 2usec    |
| > After 2 weeks of holdover  | 28 usec  | 28 usec   | 28 usec  |

Again this is based on initial power up and synced to GPS for 2 weeks

Then as long as you continue to keep the unit powered

We are well below the 100 usec specifications but it requires an initial 2 week GPS sync and then you have to keep it powered

Short GPS lock time will correct the time due to drift, but won't affect the oscillator drift rate

---

### **\*\*"Rb(Sync)" displayed on the front panel LCD**

Q. (Email from Masataka) When TFOM is more than MAX TFOM but it is not exceeded in Holdover time, "OSC" field in display of front panel indicated "Rb(Sync)" state.

Is following understand correct?

-Our understanding

This field indicate "Rb(Sync)" when following situation is existing.

- TFOM is less than MAX TFOM.
- TFOM is more than MAX TFOM but it is not exceed in Holdover time.

**A. Email from David Sohn (9 Nov 2012)** The "Rb (Sync)" indicator is not related to the TFOM and MAX TFOM checks. There is a difference between the disciplining sync state displayed there, and the overall system sync state. The overall system sync will go into holdover when TFOM exceeds MAX TFOM. Once the holdover timeout expires, the system will then transition to out of sync. However, if the input reference table entry is still valid, the disciplining system will still be attempting to synchronize and align the

system to the 1PPS reference to reduce the TFOM value. During this period, the “Rb (Sync)” indicator is asserted.

---

**Oscillator lock State name changed (changed from “Sync” to “Trk/Lock” or “Track/Lock”)**

**(Mantis Case 1880)** Version 4.8.8 update changed the reported state name, to also account for the newest Low Phase Noise Rb oscillator, also.

**Note in this Mantis case from Dave Sohn:** The new disciplining states associated with the low phase noise rubidium changed the lock state to track/lock to cover all oscillator cases. The procedure should be updated to reflect that.

## \*\*1PPS Phase Error / TFOM / MaxTFOM

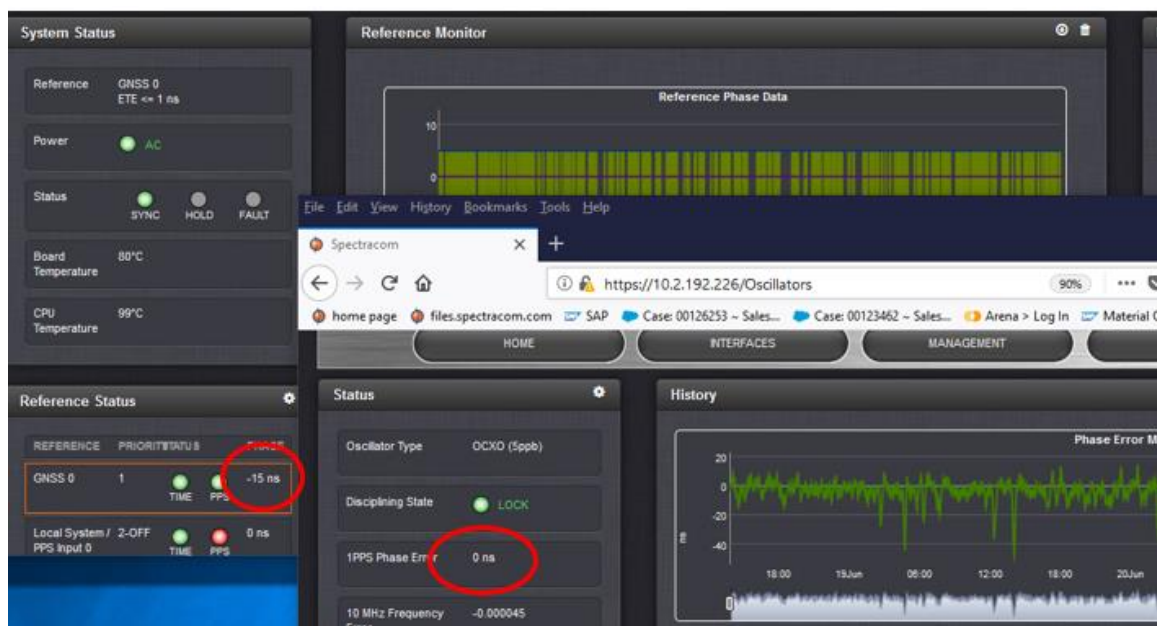
### Disciplining 1PPS Phase Error

- Estimation of 1PPS error as compared with the Reference 1PPS input.
- 1PPS Phase Error can be a positive or negative number (negative phase error)

### Notes about 1PPS Phase Error

#### 1) “Side-by-side” variances between “disciplining” phase error values (reported in the Management -> Disciplining and Reference Priority pages) versus the phase error values reported in the Tools -> Reference Monitor page

- Due to differences in granularity in the *Disciplining* -> *Reference Priority* pages, versus the *Reference Monitor* page, the phase error values for the same reference may be reported as two different values.
- As shown below, the phase error is reported as **0ns** in the *Disciplining* page, while the GPS phase error is being reported as **-15 ns** in the *Reference Monitor* page



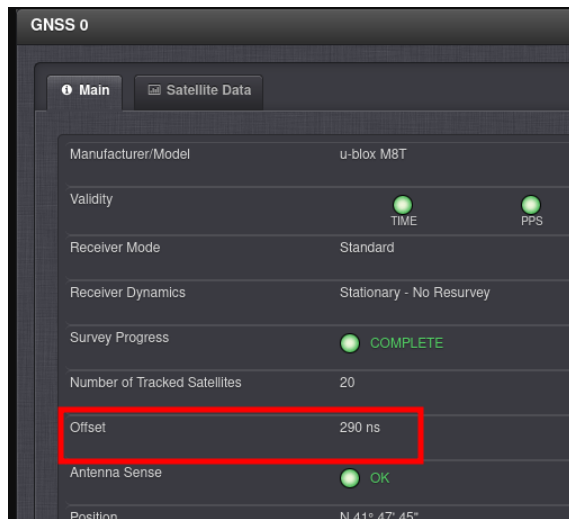
**Per Dave S (19 Jun 2018)** I don't remember the direction of the offset (negative vs positive), but as far as the differences, the disciplining phase error is a filtered error, that has higher resolution. The reference monitor phase errors are raw offset values with a 20ns resolution. They should absolutely track each other in terms of trends, but due to the filtering and differences in resolution/granularity there will be differences in the reported offsets.

#### 2) Effects on 1PPS Phase Error graphs if a GPS Offset (Cable delay) has been configured in the browser

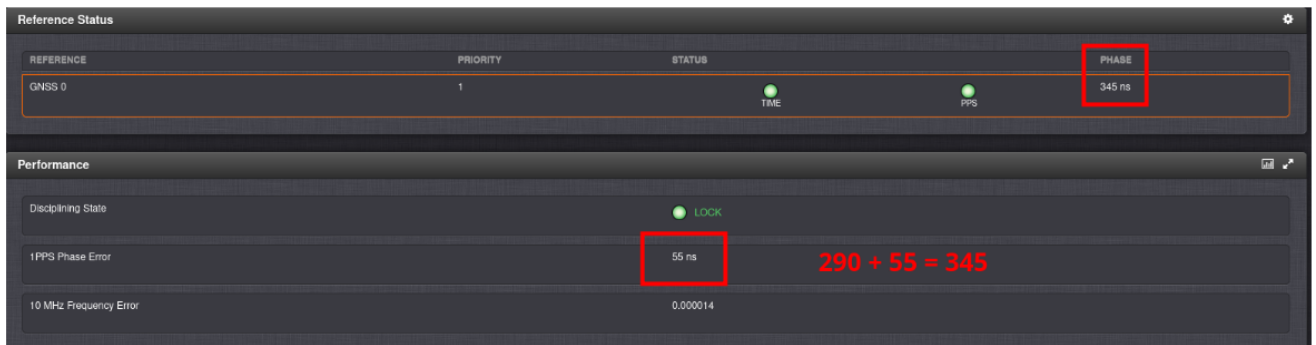
- Refer to cases such as 289423 and 255365
- Unlike the Phase Error data reported in “*log\_ref\_mon\_statuses*”, the Phase Error data in “*Log\_oscillators*” is based on **raw** (no offset applied) GPS.
- If any “**GPS Offset**” has been applied to the GPS configuration in the browser, Phase Error data reported in “*Ref Monitor*” will be offset by the value in the GPS Offset configuration (such as 800ns for instance). The Phase Error data in *Log\_oscillators* is based on raw (no offset applied) GPS.

**Example from Case 289423**

- Customer configured a **290ns** GPS cable delay/offset



Also, just to make sure I 100% understand what you're saying. You're referring to this:



Is that right? In essence, the antenna delay offset is a fixed offset and not accounted for with displaying the GNSS 0 phase of 345 ns. So the sum of the fixed offset and the actual 1PPS phase error of 55 is what we're seeing for the reference phase of 345 ns.

**Another earlier Example below (both graphs from same SecureSync) per Salesforce Case 255365**

**Email from Ron Dries (12 Jan 2021)** I looked at the logs and the sqlite data.

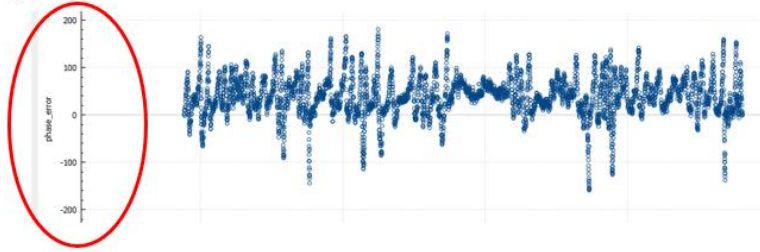
The difference between the phase error in Log\_oscillators and the phase measured in the log\_ref\_mon\_statuses is due to having an offset configured for the GPS reference.

In journal.log.1 there are entries where they set the GPS offset from 600 to 897:

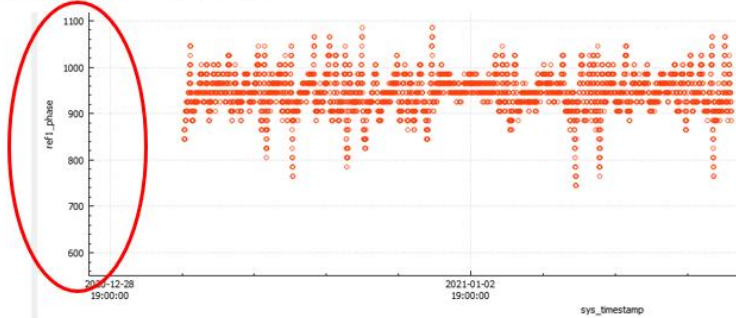
Feb 9 03:15:13 [webui] Changed Offset for GPS Reference 0 in slot 0 from GR (0)Offset: 600 to **GR (0) Offset: 897**

The reference monitor is a measurement taken before that offset gets applied

A) log\_oscillators Phase Errors



B) log\_oscillators Phase Errors



### 3) Typical phase error values

- Below are the typical expected measurements of the System PPS to UTC time. Note these are not specs, but measurement “averages” over a period of time.

#### 1 PPS Output:

|                                                | TCXO   | OCXO   | Low Phase Noise OCXO | Rubidium | Low Phase Noise Rubidium |
|------------------------------------------------|--------|--------|----------------------|----------|--------------------------|
| <b>Accuracy to UTC (1-sigma locked to GPS)</b> | ±50 ns | ±50 ns | ±25 ns               | ±25 ns   | ±25 ns                   |

**Per Dave Sohn** “These are phase error estimates carried out in SW we provide to the customer to provide general status of the performance. They are in their nature a bit conservative and so should be taken in that regard”

#### Typical discipling 1PPS phase error

- TCXO/OCXO (syncd to GPS): 10ns to 1us (TFOM 3 or 4)
- Rb (syncd to GPS): 1ns to 1us (TFOM 4)

| TFOM Value | Estimated Time Error (ETE)                             |
|------------|--------------------------------------------------------|
| 1          | $\leq 1 \text{ nsec}$                                  |
| 2          | $1 \text{ nsec} < \text{ETE} \leq 10 \text{ nsec}$     |
| 3          | $10 \text{ nsec} < \text{ETE} \leq 100 \text{ nsec}$   |
| 4          | $100 \text{ nsec} < \text{ETE} \leq 1 \text{ usec}$    |
| 5          | $1 \text{ usec} < \text{ETE} \leq 10 \text{ usec}$     |
| 6          | $10 \text{ usec} < \text{ETE} \leq 100 \text{ usec}$   |
| 7          | $100 \text{ usec} < \text{ETE} \leq 1 \text{ msec}$    |
| 8          | $1 \text{ msec} < \text{ETE} \leq 10 \text{ msec}$     |
| 9          | $10 \text{ msec} < \text{ETE} \leq 100 \text{ msec}$   |
| 10         | $100 \text{ msec} < \text{ETE} \leq 1 \text{ sec}$     |
| 11         | $1 \text{ sec} < \text{ETE} \leq 10 \text{ sec}$       |
| 12         | $10 \text{ sec} < \text{ETE} \leq 100 \text{ sec}$     |
| 13         | $100 \text{ sec} < \text{ETE} \leq 1000 \text{ sec}$   |
| 14         | $1000 \text{ sec} < \text{ETE} \leq 10000 \text{ sec}$ |
| 15         | $\text{ETE} > 10000 \text{ sec}$                       |

| TFOM Value | Estimated Time Error (ETE) (1PPS phase error)        | Notes                                                                                                                               |
|------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 1          | $\leq 1 \text{ nsec}$                                | By design, it's only possible to see TFOM 1 when an Rb oscillator is installed and the Archive software version is 4.8.8 or higher. |
| 2          | $1 \text{ nsec} < \text{ETE} \leq 10 \text{ nsec}$   | TCXO and OCXO oscillators won't ever report TFOM 2                                                                                  |
| 3          | $10 \text{ nsec} < \text{ETE} \leq 100 \text{ nsec}$ | Typical reported TFOM value for a Rb oscillator with GPS sync is TFOM 3. It's possible to see an OCXO with GPS sync report TFOM 3.  |
| 4          | $100 \text{ nsec} < \text{ETE} \leq 1 \text{ usec}$  | Typical TFOM value for TCXO/OCXO synced to GPS (may periodically go to TFOM 3)                                                      |

### TCXO/OCXO 1PPS phase error

- With TCXO or either type of OCXO oscillator installed, it takes about 20 minutes to calculate this phase error.
- Phase Errors with a TCXO/OCXO can be either positive or negative numbers.
- Like with TFOM, while the oscillator is in in Free Run, the phase error continues to increase as an estimate, based on the general characteristics of the installed oscillator (it continues to ramp up).

### Rubidium oscillator 1PPS Phase Error

- With a Rubidium oscillator installed, the oscillator reports this phase error every second.
- Phase Errors with a Rubidium oscillator will always be reported as a positive number, even if it's a negative value.
- Like with TFOM, while the oscillator is in in Free Run, the phase error continues to increase as an estimate, based on the general characteristics of the installed oscillator (it continues to ramp up).

### Typical 1PPS Phase Error values to expect:

- 1) 1PPS Phase Errors with a TCXO/OCXO can be either positive or negative numbers.
- 2) With our House reference SecureSync, low phase noise Rb synced to GPS, the 1PPS Phase Error range for 24 hours was **23** to **159**.
- 3) With the Sales demo SecureSync, OCXO, the 1PPS Phase Error range for 24 hours was **-55** to **122**
- 4) 1PPS Phase Errors with a Rb oscillator will always be reported as a positive number, even if it's a negative value

**Per Dave Sohn (15 May 2014)** Keith, I also believe the Rb error calculation is always provided as a magnitude value error, which means that regardless of whether it is actually positive or negative it is returned as a positive value.

---

## 1PPS Phase Error corrections (1PPS step sizes/period between adjustments)

### A) 1PPS Phase Error correction/step sizes with oscillator disciplining (while oscillator is locked to external 1PPS reference)

- Two questions below for Case 231847. Replies from Ron Dries (14 May 2020)

**Note:** Ron D indicated this info below applies to both OCXO and LPN OCXO oscillators

Q What is the largest automatic step (in nanoseconds) that the 10 MHz reference can make to stay disciplined to the GPS constellation's clock?

**A Keith's response:** The maximum phase change could be **~40ns per second**, if the SecureSync is adjusting for a large phase offset over a longer time period. Otherwise, in normal operation the 10 MHz is limited to changes of **0.00016 Hz**.

Q What is the minimum time period between automatic adjustments to the 10 MHz reference?

**A Keith's response:** The minimum period that an adjustment will take place once the SecureSync is locked is 120 seconds, factoring a 100 second minimum window size, and 20 seconds of settling time for the GPS reference before we make a change.

### B) 1PPS Phase Error calculations while the oscillator is in Free-Run mode

While the oscillator is in Free Run (SecureSync's in Holdover mode), the Phase Error will continue to increase (ramp up) as an estimate based on the general characteristics of the type of oscillator installed.

- Like with TFOM, while the oscillator is in in Free Run, the phase error continues to increase as an estimate, based on the general characteristics of the installed oscillator (it continues to ramp up).

---

## Report of current Phase error value

**Current 1PPS phase error value is reported in:**

- CLI command: **XO\_GetPhaseError 0** <enter>
- Newer black/charcoal web browser: [Management](#) -> [Disciplining](#) page
- Classic interface: [Status](#)-> [Time and Frequency](#) page.
- **Phase:** can be either positive or negative number.

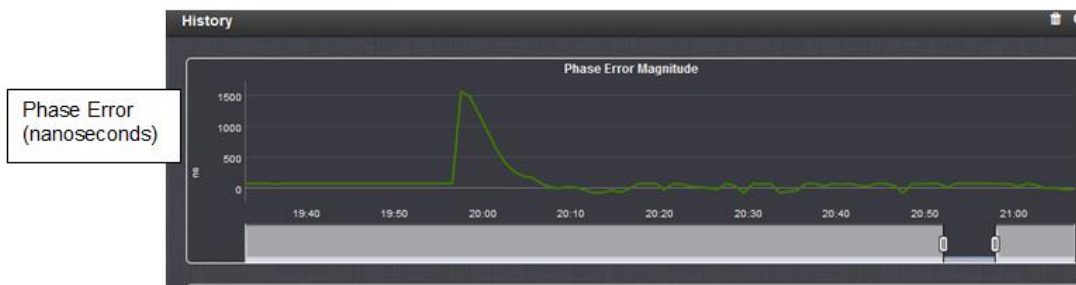
### 1. Logging phase error

- 1PPS phase error is periodically logged in the daily Discstats.log (refer to [Discstats](#))
- Example (phase error is value in bold) `16438,6082,1,0,gps0,gps0,32612,42,-1.28e-10`
- 1PPS Phase Error can also be read via the CLI using the `XO_GetPhaseError 0` command to see if on-time point is getting close to the input reference (should continue to decrease as it gets closer).
- Phase Error can be a positive or negative number (positive phase error or negative phase error)

### 2. 1PPS Phase Error graph

**Newer black/charcoal web browser v5.1.2 and above):**

[Management](#) -> [Disciplining](#) page (top graph)



- Vertical scale is dynamic
- Vertical scale (nanoseconds) is in either decimal dot or scientific notation depending on the amount of error.

The vertical scales vary depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).

**The scientific breakdown is as follows:**

- 1e-09 = 1 ns or 0000.000000001
- 1e-08= 10 ns
- 1e-07= 100ns
- 1e-06= 1 microsecond or 0000.000001000
- 1e-05= 10 microseconds 0000.000010000
- 1e-04= 100 microseconds or 0000.000100000
- 1e-03= 1 milliseconds or 0000.001000000
- 1e-02= 10 milliseconds or 0000.01000000
- 1e-01= 100 milliseconds or 0000.100000000
- 1e+00=1 second or 0001.000000000
- 1e+01= 10 Seconds or 0010.000000000
- 1e+02= 100 Seconds or 0100.000000000
- 1e+03= 1000 Seconds 1000.000000000

**Note:** If the first digit isn't a "1", multiply the first digit by the "time" value in the table above

**Examples**

- 2e-05**= 20 microseconds or 0000.000020000 ("2" times "10 microseconds" is 20 microseconds)
- 5e-06**= 5 microseconds or 0000.000050000 ("5" times "1 microseconds" is 5 microseconds)

**A) Newer web browser (v5.1.2 and above)**

**To download the raw oscillator data (not applicable to the classic interface browser)**

- Either a ".csv" or ".json" file with the oscillator values (and system temperatures) can be downloaded as desired.

**1) Download of raw oscillator data as a ".csv" file (can be opened in excel)**

- A ".csv" file can be downloaded using either of two different method (either via a download button in the Disciplining page or via a direct URL/

**CSV file download button is available in the Management -> Disciplining page of the browser**

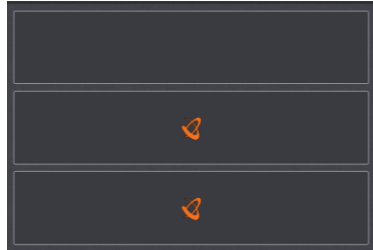
From the **Management -> Disciplining** page of the browser (click on the "down arrow" ICON on the right side of the page to download the .csv file. Press the garbage can icon to delete all the oscillator and temperature data used to display the graphs)





**Note:** The “garbage can” ICON on the upper-right corner clears/deletes all of the graph data.

**Note:** Deleting the log data will refresh the graphs.



### Manually enter the link to the OscillatorStatuslog

If you manually enter `/logs/OscillatorStatusLog.csv` after the URL of the SecureSync in the web browser, it will download a csv file that can be opened in Excel with the GPS status log data.

**Example:** <http://10.10.128.1/logs/OscillatorStatusLog.csv> (change address as applicable)

**Example .csv file output below (“Sys temp” and “CPU temp” fields were added in software version 5.3.0)**

| id    | sys timestamp    | sync | holdover | time ref | pps ref | dac   | phase error | freq error | sys temp | cpu temp | disc temp |
|-------|------------------|------|----------|----------|---------|-------|-------------|------------|----------|----------|-----------|
| 63102 | 11/18/2015 15:45 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63101 | 11/18/2015 15:43 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63100 | 11/18/2015 15:42 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63099 | 11/18/2015 15:41 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63098 | 11/18/2015 15:40 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63097 | 11/18/2015 15:39 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 99       | 0         |
| 63096 | 11/18/2015 15:38 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63095 | 11/18/2015 15:36 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63094 | 11/18/2015 15:34 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63093 | 11/18/2015 15:33 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63092 | 11/18/2015 15:32 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 99       | 0         |
| 63091 | 11/18/2015 15:31 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 80       | 100      | 0         |
| 63090 | 11/18/2015 15:30 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 100      | 0         |
| 63089 | 11/18/2015 15:29 | 0    | 0        | gps0     | gps0    | 32768 | -15         | 0          | 81       | 98       | 0         |

### Definition of fields

**Sync and Holdover:** 1 is true, 0 is false

**Time ref and PPS ref:** Selected input reference at that time

**DAC:** Oscillator’s DAC value

**Phase Error:** 1PPS Phase Error

**Freq Error:** Oscillator’s Frequency Error

**Temps: Board, CPU and Oscillator**

### Notes:

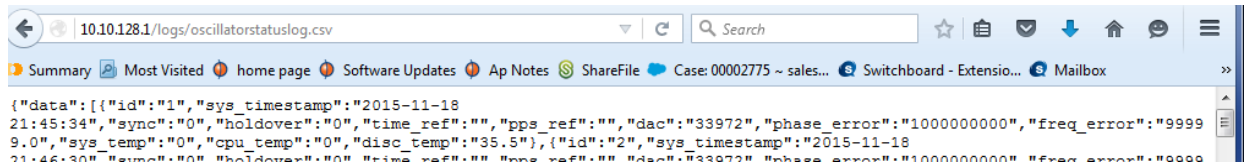
1. **Oscillator** temp is only available if sensor is installed on the main PCB
2. **Board** and **CPU** temps were added in software version 5.3.0

### B) Output of graphable oscillator and temperature data as a .json file for graphing

Same process as downloading.csv file with direct link, but replace “.csv” with “.json” instead.

If you manually enter `/logs/OscillatorStatusLog.json` after the URL of the SecureSync in the web browser it will download a json file.

**Example:** <http://10.10.128.1/logs/OscillatorStatusLog.json> (change address as applicable)

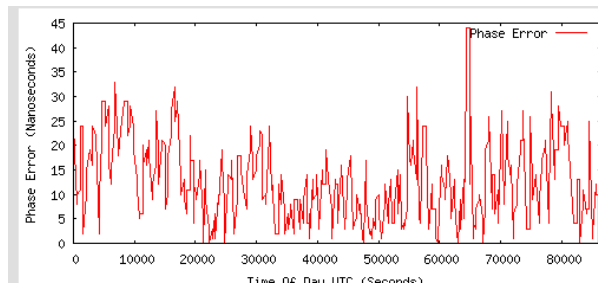


### C) "Classic Interface" browser graph

➤ **Status** -> **Disciplining** page of the browser

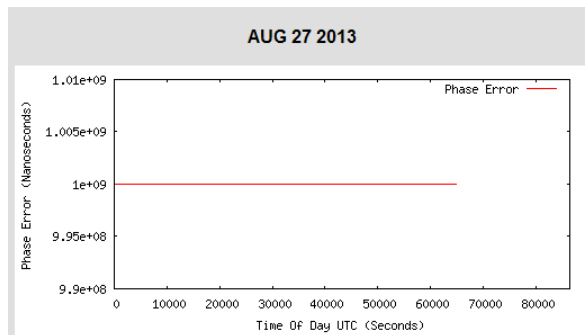
Archive Version 4.8.8 (Dec 2012, ECN 3099) added these three graphs to the **Status** -> **Disciplining** page of the browser

**Email from Dave Sohn (12/12/12)** Version 4.8.8 added phase and frequency error graphing on the unit. We generate files that include the phase and frequency errors as they are updated. Those could be pulled from the unit. We only keep the last 5 days on the box. As far as the actual logs go, we record the frequency error in the oscillator log as well.



### Analyzing phase error graph (either browser)

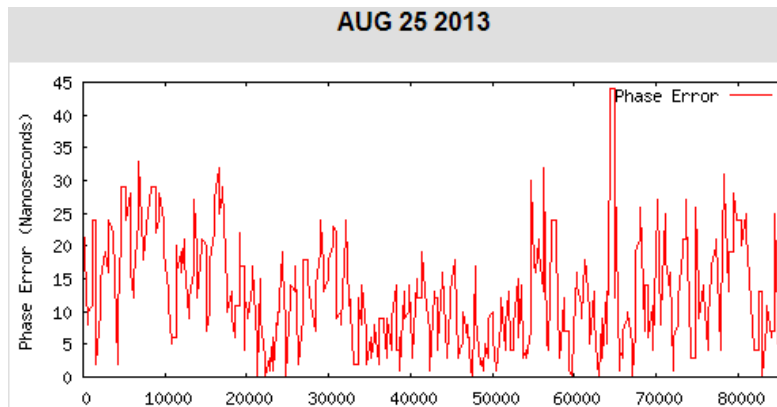
1) 10 MHz Phase Error graph showing straight line



Can be due to:

- SecureSync synced via USER/USER mode.
- SecureSync synced via NTP.
- SecureSync not synced to any reference (oscillator in free Run mode).

## B. Phase Error graph showing large intermittent spikes



### Can be due to:

- Ambient temperature changes
- Mechanical shock/vibration
- Intermittent GPS reception issues

---

## Too High/Higher than expected TFOM/Phase errors

### Conditions for higher than expected TFOM/Phase errors

#### General conditions

1. Temperature changes or high temps / issues with the cooling fan
2. **Res-SMT-GG** receiver with earlier firmware version still installed (refer to “Res-SMT-GG”:  
[..\CustomerServiceAssistance.pdf](#))
3. bad oscillator
4. Switching between input references/loss of all input references
5. Shock/Vibe
6. GPS/GNSS Receiver is in standard mode, but the unit is being used in/on a mobile platform
7. bad oscillator calibration

#### Specific conditions

##### A) With a Rubidium oscillator installed

1. **Software was downgraded from version 5.8.x (or above) back to earlier 5.7.1 (or below)**
  - Due to a change to newer method of RB oscillator disciplining in 5.8.0 (KTS disciplining the oscillator), a special EPROM patch (“**updateRbDisc.tar.gz**”) file needs to be applied to switch the Rb oscillator to start using the earlier method of disciplining (its own internal disciplining). Until the patch is applied, the oscillator will remain always in a free-run state.
    - **Link to updateRbDisc.tar.gz:** [!:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Downgrade Rb patch \(updateRbDisc.tar.gz\)](#)

## **\*\*Restart tracking / “Phase Error limit” / “Always Restart Tracking After Sync”**

**Normal 1PPS disciplining when all input references are lost for a period of time and then restored:**

- **Rubidium oscillator installed:** The Rb oscillator’s disciplining will cause the 1PPS (on-time point) from the oscillator to jump to align with the selected input reference 1PPS (not slewed over a period of time).
- **OCCO/TCXO oscillator installed:** Our Oscillator disciplining will slew the 1PPS (on-time point) from the oscillator to slew very slowly to the input reference 1PPS (not jumped to the reference).

### **A) Restart Tracking**

- Restart tracking checkbox was added in software version 4.8.6
- (Restart Tracking reportedly doesn’t work with a RB osc, though this may have changed with newer versions of software???)
- **Management** -> **Disciplining** page of the newer black web browser
- Uses the **XO\_SetMode 0 2** call.

Version 4.8.6 (June 2012) added a “Restart Tracking” capability to the **Management** -> **Disciplining** page of the web browser. When enabled, the oscillator goes back to the quickphase mode (hardware coarse adjust) one time to quickly re-align the oscillator to the PPS reference. Then, this field goes back to disabled. This needs to be performed each time it’s desired to snap the PPS to the reference.

| New State      | State Value | Meaning                                                                            |
|----------------|-------------|------------------------------------------------------------------------------------|
| Warm-Up        | 1           | At startup/reset. Will stay in this state until a valid time reference is received |
| Calibrate      | 2           | Osc calibration done after startup/reset once a valid reference is found           |
| Tracking Setup | 3           | Quick phase/Qualification.                                                         |
| Tracking Lock  | 4           | Locked into time reference. Constant fine tuning during this state.                |
| Free Run       | 5           | Time reference has been lost. Using oscillator accuracy during holder.             |

**Note:** There was a Disciplining State value 6 at one time. But it was removed in an earlier version of software.

### **When performing a Restart Tracking**

If you have a valid time reference connector to the board, the state should go from “1” to “4”, “4” indicating it has locked in to the reference. If you were to remove the time reference, the state would go to “5” indicating that the unit was now in holdover mode.

**When the unit is in state “4”, you should see the state change to “3” indicating that the unit is in the quick phase state and that the tracking has restarted.**

**Email from Keith (27 Jul 2015)** Thanks for reporting what you are observing (or possibly were observing but no longer, by now) after connecting a new antenna. This is initially expected operation after connecting an antenna. The time it takes to clear the alarm thereafter, unless the unit is power cycled is dependent on how long it’s been without an antenna

Once the SecureSync syncs to GPS after each power-up, it starts to adjust the oscillator. if power cycled/rebooted, it first snaps it in close with a hardware adjustment. Then it switches to very slow slewing via software. If it’s not power cycled, It continues to slowly slew the oscillator until its re-aligned to GPS. During this whole time, the Frequency Error Alarm is asserted. Typically, around 15 to 30 minutes after the SecureSync goes into sync to GPS, the oscillator’s frequency is aligned very closely to 10 MHz (based on the GPS receiver’s 1PPS signal), which causes the Frequency Error alarm (and associated Fault LED) to clear. But if it’s been running a while without GPS, it can take a few hours for the Frequency Alarm to clear,

In lieu of power cycling the unit, you can also manually perform a “restart tracking” which speeds up this alignment (it is similar to a reboot as far as the oscillator is concerned with the oscillator once-again coarse adjusted to the 1PPS reference even though no reboot was actually performed).

To perform a restart tracking, navigate to the **Management** -> **Disciplining** page of the browser. On the left-side of the page, click on the “gear” icon to the right of “Status”. In the pop-up window, select **Restart Tracking** and then press Submit.



The oscillator will now be realigned much faster to the GPS signal. The Frequency Error alarm should typically clear within about 15 to 30 minutes after performing this step.

Note this coarse adjust process without a reboot is a “one-time” event. The Restart Tracking checkbox doesn’t remain selected and a Restart Tracking will not be performed again, unless a user manually performs the same process again.

---

## Associated Log entries for Restart Tracking

### 1) Journal log entry for restart tracking being commanded

*Example entry below*

Aug 6 11:46:22 Spectracom Spectracom: [webui] Changed Mode for Oscillator in slot 0 from XO Mode: 0 to XO Mode: 2

### 2) Timing log entry for Restart Tracking occurring

*Example entry below*

Aug 6 13:57:33 Spectracom Spectracom: [system] 2013 218 13:57:33 000 **Oscillator control: Reset.**

---

## Restart tracking performed while in Holdover mode (oscillator free-run)

(based on testing Keith performed with OCXO and v5.8.9)

- TFOM changed from its starting value (such as TFOM 3) to a value such as TFOM 5 (doesn't go to TFOM 15)
- DAC went to “32852”
- Stays in “Free-Run” and “TFOM 5” till input reference is restored
- 1PPS Phase Error jumped to like 2500ns/2600ns and rapidly climbed to like 3400ns

---

## Restart tracking not working (no DAC change or shift in 1PPS after issuing command)

- 1) Is a Rb oscillator installed? (Restart Tracking reportedly doesn't work with a RB, though this may have changed with newer versions of software???)
- 2) Make sure an external input reference is present and valid.
- 3) With NTP input, software version needs to be version 5.3.0, which implemented host disciplining

## B) B) Phase Error limit field (versions 5.2.0 and above)

- New feature added in version 5.2.0 (newer black/charcoal browser).
- Refer to online SecureSync user guide [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/OscConfiguring.htm?Highlight=restart%20track](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm?Highlight=restart%20track)
- Not available in the “classic interface” browser

**Management** -> **Disciplining** page, Status gear icon pop-up window



**Phase Error Limit field** was added to the Edit window of the Disciplining page allowing for an automatic disciplining tracking restart, once the phase error limit is exceeded, thus avoiding manual intervention.

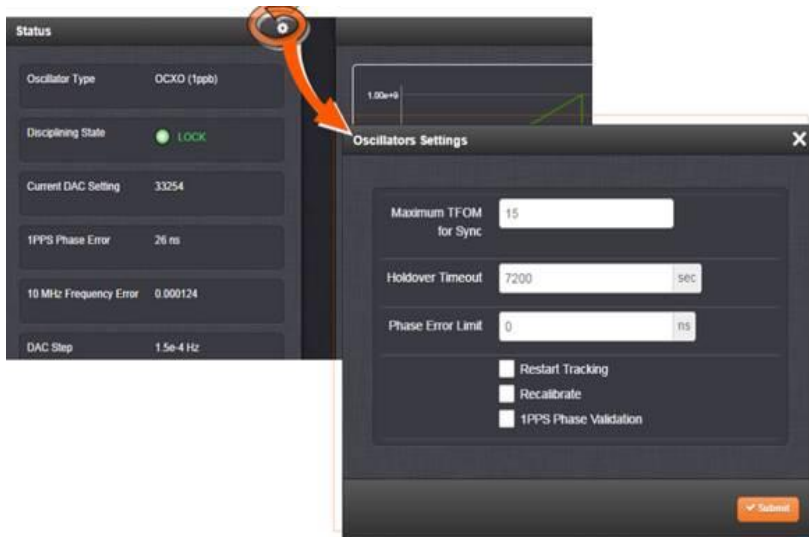
### 1PPS Phase Error exceeds Phase Error Limit

- Osc.log entry asserted
- Automatic restart Tracking occurs
- Don't believe any alarms are asserted

**Email Keith sent (5 Aug 15) covering info on both “Restart Tracking” and “Phase Error Limit”**

**For more info on Restart tracking and./or Phase Error Limit, please refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/OscConfiguring.htm?Highlight=restart%20track](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm?Highlight=restart%20track)**

To either manually or automatically expedite the oscillator lock/relock, navigate to the **Management** -> **Disciplining** page of the browser. On the left side of the page, click on the Gear icon to the right of “Status”. This will open a pop-up window (as shown below). Selecting the “Restart Tracking” checkbox at the bottom will start a “one-time” oscillator relocking (the same process as occurs the first time after each reboot that an external reference is applied). This process is only performed when a user selects this checkbox (it can be applied multiple times/whenever desired as long as there is an external reference available for it to lock to).



To alleviate manual intervention, the “Phase Error Limit field” in this same window is used to perform an “automatic Restart Tracking” whenever the 1PPS phase error (the offset between the internal 1PPS and the external input’s 1PPS) exceeds a user-specified value. For instance, if the Phase Error limit is set to 1000ns, if the internal 1PPS is more than 1000ns different than the external 1PPS input, a “restart tracking” is performed at that time. Instead of slowly slewing 1000ns, the oscillator is hardware re-aligned to the reference, just like when a user manual initiates a “Restart Tracking”.

## Associated Log entries for Phase Error Limit

### 1) Journal log entry for “Phase Error Limit” being configured

*Example entry below*

“Changed Phase Error Limit for Oscillator in slot 0 from XO Phase Error Limit: 0 ns to PhaseErrorLim value: 300 ns”

### 2) Osc.log entry for Phase Error Limit being exceeded/function occurred

*Example entry below*

```
2020 288 06:55:37 000 XO1: Disciplining restart from phase error limit
2020 288 06:57:43 000 XO1: Start Phase Err: +165.0
2020 288 06:58:43 000 XO1: DAC Setting: 0x71F3
2020 288 06:58:43 000 XO1: End Phase Err: +310.0
2020 288 06:58:43 000 XO1: Freq Err: +0.000000
2020 288 06:58:43 000 XO1: Err Std Dev: +49.9
```

## Delays between auto Restart Trackings occurring (if Phase error Limit remains exceeded even after restart Tracking occurs)

**Q from Keith to Ron D/Dave S and Gary B (13 May 2022)** Is there an automatic delay between how often the Phase Error limit will cause Restart Tracking? If the Phase Error limit is set to "5ns" for instance, and the Phase Error remains above 5ns, even after Restart Tracking, should it go into a continuous loop of Restart tracking.? On this unit with beta 5.9.5 installed, Phase error limit still set to 5ns, Phase Error 56ns, but unit isn't performing another Restart Tracking. Is this expected?

Update from Keith (same day): At least with an RB installed, it appears Restart Tracking will re-occur about every 13 minutes or so, if Phase Error Limit remains exceeded:

osc Log 🔄

Search: restart

| Id  | Date            | Entity   | Message                                                                |
|-----|-----------------|----------|------------------------------------------------------------------------|
| 626 | May 13 15:43:57 | [system] | 2022 133 15:43:57 000 XO1: Disciplining restart from phase error limit |
| 616 | May 13 15:30:55 | [system] | 2022 133 15:30:55 000 XO1: Disciplining restart from phase error limit |
| 608 | May 13 15:17:52 | [system] | 2022 133 15:17:52 000 XO1: Disciplining restart from phase error limit |



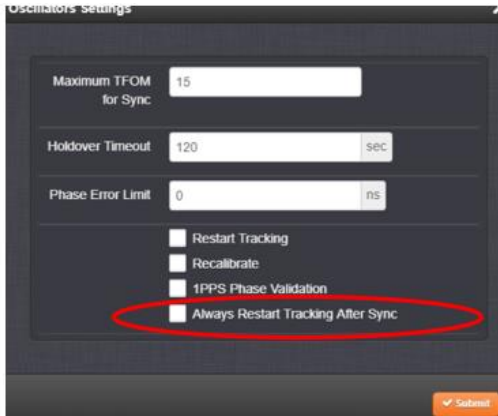
---

---

C) “Always Restart Tracking After Sync” checkbox (versions 5.8.9?? and above)

- Refer to the online SecureSync user guide at: update [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/OscConfiguring.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm)
- Added in update v5.8.9??

*Management* -> *Disciplining* page, Status gear icon pop-up window



*Except from online SecureSync userguide*

**Always Restart Tracking After Sync:** When selected, this option will ensure that every time the unit exits holdover, the discipline tracking is restarted. It should be noted that this setting will only restart the tracking once when using the Phase Error Limit, unless the unit re-enters holdover.

**Associated Log entries for “Always Restart Tracking After Sync” checkbox**

- 1) Journal log entry for “Always Restart Tracking After Sync” being configured

*Example entry below*

---

## TFOM (Time Figure Of Merit)

### Report of current TFOM value

1. Reported on left side of the [Management](#) -> [Disciplining](#) page
2. Reported with the **SS\_GetTfom 0** command
3. Reported at the end of the **status** CLI command (in conjunction with the configured MaxTfom value)

Q. How does the SecureSync calculate the TFOM Value?

A. modified **reply from Keith (26 Jun 14)** The SecureSync uses the calculated phase error value as the input for the TFOM Calculation. This data is collected in a variable size window and the result compared to a table of set values to select the TFOM value.

The variable min and max measurement window gets complex. It is set depending on the accuracy of the reference source, the stability of the data and the type of oscillator used.

The TFOM is an estimate of the timing error of the board and meant to be used as an indicator of the general performance of the timing;

The Time Figure of Merit (TFOM) enumeration is defined to provide a dimensionless quality measure of the overall time/1PPS synchronization based on an Estimated Time Error (ETE). This measure is used for overall sync status of our clock to the internal 1PPS. Our synchronization definition is derived from our use of time and 1PPS to achieve both synchronization of time and synchronization of frequency.

### Here's some information about TFOM for you:

In summary, a TFOM change from 3 to a 4 does not necessarily indicate any problems. You just want to make sure the front panel Sync LED is still green. If it's not solid green, the TFOM will slowly increase until the NetClock is back in sync again. It may have likely been at the top end of the range for a TFOM of 3, changed slightly and therefore became a TFOM of 4 (refer to the table further below). This is normal operation.

The TFOM value is really a factor of the type of oscillator installed and the stability/accuracy of the selected input reference that the SecureSync is synced to (With GPS typically being the best external reference for synchronization). TFOM values of 3 and 4 are expected values to see, when a TCXO or OCXO oscillator is installed and when it's synced to GPS. TFOMs are usually lower with a Rubidium oscillator installed, as long as the SecureSync is in sync.

The Time Figure of Merit (TFOM) enumeration is defined to provide a dimensionless quality measure of the overall time/1PPS synchronization based on an Estimated Time Error (ETE). This measure is used for overall sync status of internal 1PPS to the input reference 1PPS. Our synchronization definition is derived from the use of time and 1PPS to achieve both synchronization of time as well as synchronization of frequency.

**Email from Dave Sohn (11/9/12)** TFOM / ETE is a logarithmic scale of phase error to provide a high level view of the phase error magnitude. The phase error calculated is translated directly to a TFOM value using the table below, where the phase error falls in the ETE column (Table 4-1 in the user manual). The system determines phase differences and frequency differences between the input 1PPS reference and our system 1PPS based on our accurate system oscillator.

The TFOM (Time Figure of Merit) value is a very accurate comparison (Estimate- not a measurement) of the input reference 1PPS versus the 1PPS output from the oscillator disciplining circuit (which uses the input 1PPS as its reference). As the SecureSync is able to discipline itself to a very stable and accurate 1PPS, the TFOM values will decrease. However, if the input reference 1PPS is jittery or does not have a "crisp" rising edge that it can definitively define as the trigger point, each time the TFOM is calculated, the value is going to be higher than expected.

The current **TFOM value** can be viewed in the **Status** -> **Time and Frequency** page.

**Note:** As of at least version 5.1.7, TFOM values are not logged.

**Phase Accuracy error** can be viewed to see if on-time point is getting close to the input reference (should continue to decrease as it gets closer). The current 1PPS **Phase Error** can be viewed in the **Status->Time and Frequency** page.

## TFOM Table for SecureSyncs

| TFOM Value | Estimated Time Error (ETE) (1PPS phase error)          | Notes                                                                                                                                                                                                                                                                                                         |
|------------|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1          | $\leq 1 \text{ nsec}$                                  | Starting in <b>upgrade version 5.1.3</b> (improved disciplining), it's now possible for all oscillator types, any input reference, to report TFOM 1 and 2<br>Prior to version 5.1.3, it's only possible to see TFOM 1 when an Rb oscillator is installed and the Archive software version is 4.8.8 or higher. |
| 2          | $1 \text{ nsec} < \text{ETE} \leq 10 \text{ nsec}$     | Starting in upgrade <b>version 5.1.3</b> (improved disciplining), it's now possible for all oscillator types, any input reference, to report TFOMs 1 and 2.<br>Prior to version 5.1.3, TCXO and OCXO oscillators won't ever report TFOM 2                                                                     |
| 3          | $10 \text{ nsec} < \text{ETE} \leq 100 \text{ nsec}$   | Typical reported TFOM value for a Rb oscillator with GPS sync is TFOM 3.<br>It's possible to see an OCXO with GPS sync report TFOM 3.                                                                                                                                                                         |
| 4          | $100 \text{ nsec} < \text{ETE} \leq 1 \text{ usec}$    | Typical TFOM value for TCXO/OCXO synced to GPS (may periodically go to TFOM 3)                                                                                                                                                                                                                                |
| 5          | $1 \text{ usec} < \text{ETE} \leq 10 \text{ usec}$     |                                                                                                                                                                                                                                                                                                               |
| 6          | $10 \text{ usec} < \text{ETE} \leq 100 \text{ usec}$   |                                                                                                                                                                                                                                                                                                               |
| 7          | $100 \text{ usec} < \text{ETE} \leq 1 \text{ msec}$    |                                                                                                                                                                                                                                                                                                               |
| 8          | $1 \text{ msec} < \text{ETE} \leq 10 \text{ msec}$     |                                                                                                                                                                                                                                                                                                               |
| 9          | $10 \text{ msec} < \text{ETE} \leq 100 \text{ msec}$   |                                                                                                                                                                                                                                                                                                               |
| 10         | $100 \text{ msec} < \text{ETE} \leq 1 \text{ sec}$     |                                                                                                                                                                                                                                                                                                               |
| 11         | $1 \text{ sec} < \text{ETE} \leq 10 \text{ sec}$       |                                                                                                                                                                                                                                                                                                               |
| 12         | $10 \text{ sec} < \text{ETE} \leq 100 \text{ sec}$     |                                                                                                                                                                                                                                                                                                               |
| 13         | $100 \text{ sec} < \text{ETE} \leq 1000 \text{ sec}$   |                                                                                                                                                                                                                                                                                                               |
| 14         | $1000 \text{ sec} < \text{ETE} \leq 10000 \text{ sec}$ |                                                                                                                                                                                                                                                                                                               |
| 15         | $\text{ETE} > 10000 \text{ sec}$                       | Max TFOM 15 is the factory default setting. With MaxTFOM set to 15, MaxTFOM is never exceeded.                                                                                                                                                                                                                |

### Notes about TFOM

- TFOM value is updated:
  - About once-per-second with a Rubidium oscillator
  - About every 10 seconds with a TCXO or either type of OCXO oscillator installed. This is the amount of time it takes for the TFOM value to be calculated.
- The TFOM is a calculated phase error between the reference 1PPS vs the disciplined 1PPS. With an RB, the oscillator reports this phase error every second. With an OCXO it takes about 10 minutes to calculate this phase error.
- The calculated TFOM also adds on any correction applied in order to phase align the disciplined 1PPS to the 10 MHz from the oscillator. As corrections are made for this continuous alignment the amount of error correction are applied to the TFOM.
- TFOM is a worst-case error measurement. It may be better than the measured error, but it won't be any worse the measured error.
- TFOM with an OCXO oscillator installed will be no less than 3 (never 1 or 2) because of values intentionally added to the measurements if they are "too good" for what is expected to be measured with an OCXO. This is to make sure the TFOM will be no less than 3 with the OCXO oscillator (Since we sample for very short periods of time, the values read may be VERY good during that time frame, but too good to be expected, so we throw in a correction factor so that the calculated TFOM isn't BETTER than what the realistic values are.

- TFOM with an Rb oscillator, synced to GPS should have a TFOM value of 3. It may on occasion go to a value of 2 for short periods of time, but for the most part, it should be a value of 3.
- 

## Known issues with TFOM/High TFOM

### TFOM 1 with no input reference

- (Refer to Mantis case 1933)
- Version 4.8.8 allows TFOM to be a “1” with a Rb oscillator installed, even without SecureSync being synced to a reference.

### High TFOM (~TFOM 8) with Rb oscillator and software versions 5.8.0 thru 5.8.4

#### RB oscillator potentially stuck in warm-up mode (applicable to versions 5.8.0 through 5.8.4)

**Summary:** Rubidium oscillators being disciplined by KTS (instead of internally, versions prior to 5.8.0) starting in 5.8.0, can potentially stay in warm-up mode after initial power-on. This causes very high TFOM (such as TFOM 8), from that point forward

- Refer to case 208069 (for Northrop Grumman)
- Applicable to versions 5.8.0 thru 5.8.4 (fixed in 5.8.5)
  - Issue fixed in version **5.8.5** (per 5.8.5 Release Notes: “Modified Rubidium disciplining support to prevent breaking from the warm-up state early”)

---

## Time stamp for the last time the TFOM value changed to another number

Starting in Archive version 4.8.7, the **Status -> Disciplining** page of the browser also indicates the time stamp of the last time TFOM value changed to a different value (it doesn't display what TFOM it changed to- just that it changed at the specified date/time).

If the date/time stamp was three days ago, it's been the current TFOM value (as reported in the Status -> Time and Frequency page of the web browser) for the last three days straight (hasn't gone up or down, since the timestamp shown).

---

## Desire to remotely monitor TFOM values:

(15 Nov 2012 KW) The TFOM values are not currently logged, but they can be monitored remotely, if desired.

- Via the web browser.
- Via the CLI interface using the tfomget command
- Via an SNMP Get (from an SNMP Manager on the network). The SPECTRACOM-SECURESYNC-MIB file defines this (Refer to “ssSysStaTfom” in this MIB file)
- Set MaxTFOM to a value other than 15. Then, send an email and/or SNMP trap when the TFOM exceeds the MAXtfom value. The **“1PPS Not in Specification”** alarm is asserted when this condition occurs. There is an available trap and/or email associated with this alarm. When TFOM is no longer exceeded, the “1PPS restored to Specification” log entry, and associated email/trap can indicate this.

## Desire to remotely monitor (and record) TFOM values:

The TFOM value can also be polled via the tfomget CLI command. This command can be issued via telnet/SSH or via direct connect to the front panel DB9 SERIAL port. Using HyperTerminal, Procomm or Terraterm, (9600 baud, 8 bit, 1 Stop bit, No parity) issuing this command will return the TFOM. Refer to the attached HyperTerminal Application Note

for info on this connection. I know with at least HyperTerminal, you can create a simple .txt file with nothing but this command in it. Then, in HyperTerminal, perform a Transfer -> Send Text File. HyperTerminal will continue to send the command until it has gone through the entire list (to make the list of this command huge, copy all and paste. This doubles the entries in the file, each time. Refer to the attached txt document.

HyperTerminal can also log all of the responses to this command (**Transfer -> Capture Text**).

### Notes about remote monitoring of SNMP

- 1) Refer to the SNMP Application Note for more info on using SNMP to monitor TFOM.
- 2) Starting in Archive version 4.8.7, the **Status -> Disciplining** page of the browser also indicates the time stamp of the last time TFOM value changed to a different value (it doesn't display what TFOM it changed to- just that it changed at the specified date/time).

If the date/time stamp was three days ago, it's been the current TFOM value (as reported in the **Status -> Time and Frequency** page of the web browser) for the last three days straight (hasn't gone up or down, since the timestamp shown).

---

### Notes about TFOM

- 1) The TFOM is a calculated phase error between the reference 1PPS vs the disciplined 1PPS.
- 2) With a Rubidium oscillator installed, the oscillator reports this TFOM error every second.
- 3) The TFOM value is recalculated/updated about every 20 seconds or so.
- 4) The calculated TFOM also adds on any correction applied in order to phase align the disciplined 1PPS to the 10 MHz from the oscillator. As corrections are made for this continuous alignment, the amount of error correction is applied to the TFOM.
- 5) TFOM is a worst-case error measurement. It may be better than the measured error, but it won't be any worse than the measured error.
- 6) **TFOM with an OCXO oscillator** installed will be no less than 3 (never 1 or 2) because of values intentionally added to the measurements if they are "too good" for what is expected to be measured with an OCXO. This is to make sure the TFOM will be no less than 3 with the OCXO oscillator (Since we sample for very short periods of time, the values read may be VERY good during that time frame, but too good to be expected, so we throw in a correction factor so that the calculated TFOM isn't BETTER than what the realistic values are.
- 7) **TFOM with an Rb oscillator** installed and with SecureSync synced to GPS, should have a TFOM value of 3. It may on occasion go to a value of 2 for short periods of time, but for the most part, it should be a value of 3.
- 8) **Note: (Per Dave Sohn)** Rubidium may take some time to settle into a low TFOM as it runs through disciplining.
- 9) **Note:** Starting in Application v4.8.8, TFOM can now be a "1" when a Rubidium oscillator is installed.
- 10) TFOM with no input reference after power-up will remain at 15, until an external reference becomes available.
- 11) The TFOM after all valid input references have been removed or declared no longer valid (Sync status was true) will initially stay at the TFOM value it was when the input references were no longer valid and will start to increment from there, based on the typical drift rates for the type of oscillator installed (If it was a 3, it will increment to a 4, etc).
- 12) The table above is the breakdown of the TFOM values to the corresponding Estimated Time Errors, based on the reported TFOM value:
- 13) High TFOM when using EPP0 (External 1PPS input)

- 14) The most common issue we see when customers use an external 1PPS input ("EPP0") as the 1PPS input reference is due to ringing of the signal because of improper termination. The input impedance of the 1PPS signal is high impedance. However, the 1PPS source may desire a 50 ohm termination into the TSync-PCIe-PCIe board (instead of high impedance). If the source desires a 50 ohm load termination, the input 1PPS may likely "ring" inside of the TSync-PCIe board. The ringing of the 1PPS signal prevents a "crisp" point at which the TSync-PCIe board can trigger on. With ringing of the signal present, the detected trigger point may coincidentally be at the right point, but it could also trigger too early or too late. So, with each 1PPS input when the signal is ringing, it may trigger at a different point on the signal each time. This prevents the disciplining circuit from being able to receive a stable 1PPS that is can accurately discipline to, and so the TFOM values will also be much higher than expected.
- 15) We have seen a few other similar cases where an external 1PPS input was causing a jittery 1PPS input because of improper termination of the signal at the input of the board. These were all resolved with a 50 ohm input being applied. To see this affect, if you have access to an oscilloscope, input the 1PPS signal from the source with a high input impedance setting on the scope. Look at the rising edge. You will likely see a ringing of the signal with no defined rising edge. Then, switch the scope to 50 ohm termination and you will likely notice the signal a become a crisp 1PPS with a very defined rising edge. This is what the board is also likely receiving and seeing, as well. To prevent the ringing of the 1PPS input from occurring and affecting the TSync-PCIe-PCIe board, terminate the 1PPS input from the source with a 50 ohm load resistor. This will often "clean up the signal" so that it can be a better reference into the board.
- 16) Let me know if adding the 50 ohm resistor from the input to ground allows the TFOM values to significantly decrease (TFOM values of 3 or 4 would be expected). For your information, the TFOM value is recalculated/updated about every 20 seconds or so.

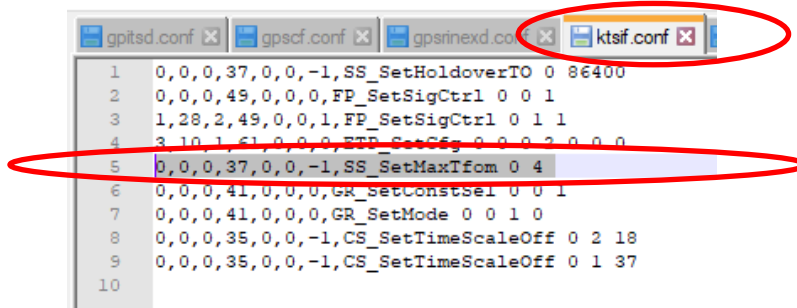
## MaxTFOM (Max TFOM / “Maximum TFOM for Sync”)

### Configuring MaxTFOM (Maximum TFOM for Sync)

**Note:** info on TFOM exceeding MaxTFOM is further below.

#### Configuration file for MaxTFOM value

MaxTOM value for the black/charcoal web browser is stored in the ktsif file.



#### A) Via CLI commands

- MaxTFOM should be able to both read/set via REST API
- MaxTFOM cannot be **set** (configured) via the CLI (must be configured via the browser)
- Configured MaxTFOM value can be **reported** (not set, due to CLI permissions) via CLI using either the **SS\_GetMaxTfom 0** command or with the **status** command (which reports both the MaxTfom value as well as the current TFom value, as shown below):

```
spadmin@Spectracom ~ $ status
REF:T=ptp0 P=ptp0
NTP:Strat=16 Sync=N
OSC:OCYO (Trk/Lock)
TFOM=10 MaxTFOM=15
spadmin@Spectracom ~ $
```

(email from Keith 14 Sep 17) A short note for you regarding the SecureSync's "1PPS not in Specification" alarm being asserted (due to the TFOM value exceeding the MaxTFOM value). You may find this additional info below helpful in the future.

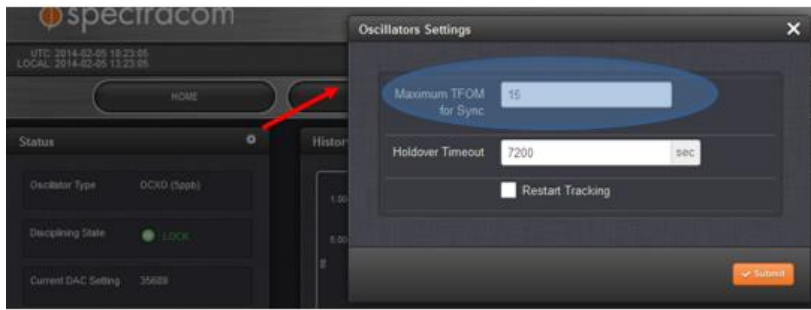
FYI- instead of needing to check the current TFOM and the MaxTFOM values via the browser, there is a convenient CLI command which will simultaneously report both the current TFOM value and the configured MaxTFOM value (there is a separate command available for each of these two values but this one command reports both at the same time).

Typing the CLI command of status <enter> will respond with both the current TFOM value, and the currently configured MaxTFOM value (as shown below). If the current MaxTFOM value is set to "3", while the TFOM value is a "4". the unit's MaxTFOM value just needs to be changed to a "4" instead. The MaxTFOM value can be changed via the **Management > Disciplining** page of the browser.

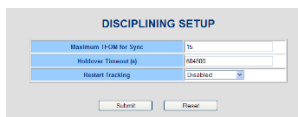
#### B) Via Newer browser (Archive versions 5.1.2 and above)

- The MaxTFOM (Maximum TFOM for Sync") value is configured in the **Management -> Disciplining** page of the browser, and then clickon the "gear" next to "Status"

Note the "MaxTFOM" field is configured in the **Management -> Disciplining** page of the newer (black/charcoal) web browser. As shown below, click on the gear icon to the right of "status" (on the left side of the page). The MaxTFOM field can be configured in the pop-up window that opens. Press Submit after changing this value.



### C) Archive versions 5.0.2 and below (classic interface browser)



- When current TFOM value exceeds Max TFOM, SecureSync will go into “Holdover” mode, until TFOM falls below Max TFOM.

**Important note:** The input reference is still used to discipline the oscillator while TFOM is exceeding MaxTFOM. So it's not truly in “Holdover” mode. It's just reported as being in “Holdover”, until MaxTFOM is no longer exceeded.

**TIME AND FREQUENCY STATUS**

|                                |                     |
|--------------------------------|---------------------|
| Selected Time Reference Source | GPS 0               |
| Selected 1PPS Reference Source | GPS 0               |
| Synchronization                | OK                  |
| Holdover                       | In Holdover         |
| Time Figure of Merit (TFOM)    | 2                   |
| Estimated Time Error (ETE)     | 1 ns < ETE <= 10 ns |
| Timescale Reference            | UTC                 |
| Oscillator Type                | OCXO (5ppb)         |
| Oscillator State               | Track/Lock          |
| 1PPS Phase Error (ns)          | 2                   |
| 10MHz Frequency Error          | 1.27e-10            |

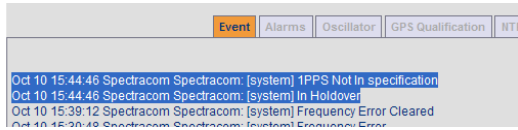
**REFERENCE STATUS**

| Reference    | Time      | 1PPS      |
|--------------|-----------|-----------|
| GPS 0        | OK        | OK        |
| NTP          | Not Valid | Not Valid |
| User         | Not Valid | Not Valid |
| Local System | OK        | OK        |

| Event                                                                     | Alarms | Oscillator | GPS Qualification | NTP |
|---------------------------------------------------------------------------|--------|------------|-------------------|-----|
| Oct 10 15:44:46 Spectracom Spectracom: [system] 1PPS Not In specification |        |            |                   |     |
| Oct 10 15:44:46 Spectracom Spectracom: [system] In Holdover               |        |            |                   |     |
| Oct 10 15:39:12 Spectracom Spectracom: [system] Frequency Error Cleared   |        |            |                   |     |
| Oct 10 15:39:49 Spectracom Spectracom: [system] Frequency Error           |        |            |                   |     |



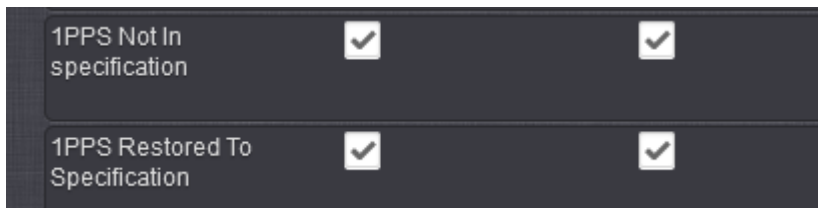
- When TFOM exceeds MaxTFOM, “1PPS not in Specification” alarm is asserted. See note further below.



- When MaxTFOM is no longer exceeded, “1PPS Restored to Specification” is asserted. See note further below.
- (not applicable to the Rb oscillator) When current TFOM exceeds Max TFOM, OCXO/TCXO oscillator disciplining occurs faster.

## When TFOM exceeds MaxTFOM (“Maximum TFOM for Sync”) / 1PPS not in Specification

- Forced Holdover mode/Holdover alerts are asserted
- “1PPS not in Specification” alarms asserted. (SNMP alerts sent, if enabled)



- TCXO and OCXO disciplining rates are altered to help expedite the lowering of TFOM.

**Important note:** The input reference is still used to discipline the oscillator while TFOM is exceeding MaxTFOM. So it's not truly in “Holdover” mode. It's just reported as being in “Holdover”, until MaxTFOM is no longer exceeded

The “TFOM” (Time Figure of Merit) field defines the largest TFOM value (TFOM is SecureSync's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors - known as the estimated time error or “ETE”) that is allowed before disciplining is no longer performed on the oscillator. The larger the TFOM value, the less accurate SecureSync believes it is aligned with its 1PPS input referenced that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available MaxTFOM range is 1 through 15.

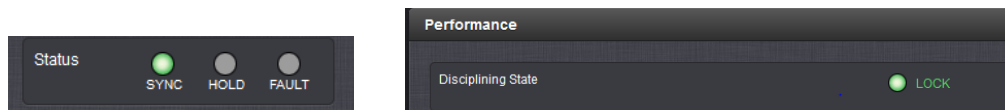
## OCXO and TCXO disciplining rates when TFOM exceeds MaxTFOM

The two rates below do not apply to the Rb oscillator disciplining. There is no difference in the maximum rate of phase alignment based on TFOM during Rubidium disciplining.

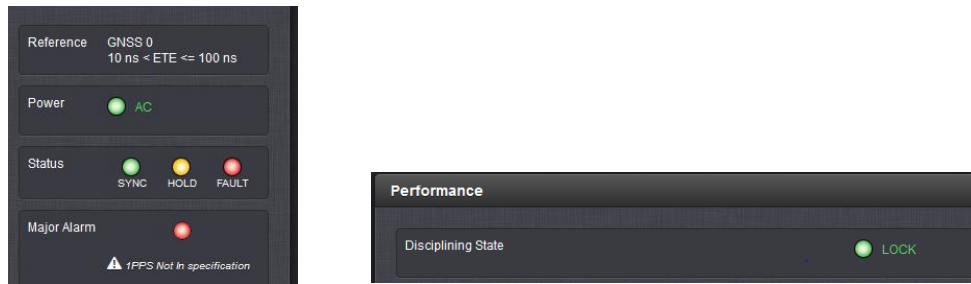
- If the current TFOM value is less than or equal to the Max TFOM setting, the frequency of the oscillator is offset by a maximum of 0.4 Hz (40 ns/s) until the 1PPS is realigned.
- If the current TFOM value is more than the Max TFOM setting, the frequency of the oscillator is offset by a maximum of 4 Hz (400 ns/s) until the 1PPS is realigned.
- MaxTFOM is configured / viewed in the [Setup->Disciplining](#) page.
- MaxTFOM can be viewed in the [Status->Time and Frequency](#) page.
- **Default MaxTFOM** is 15 (TFOM never exceeds Max TFOM).
- If MaxTFOM is set to less than 15, User/User mode will not allow SecureSync to go into Sync.

## Holdover mode (Holdover indicator turns solid yellow when 1PPS Not in Specification)

**A) RB oscillator. Tracking sats. MaxTFOM set to default “15”. TFOM is 2 (TFOM 2 not exceeding MaxTFOM 15)**



**B) RB oscillator. MaxTFOM changed to “1”. TFOM is 2 (TFOM 2 is now exceeding MaxTFOM 1)**



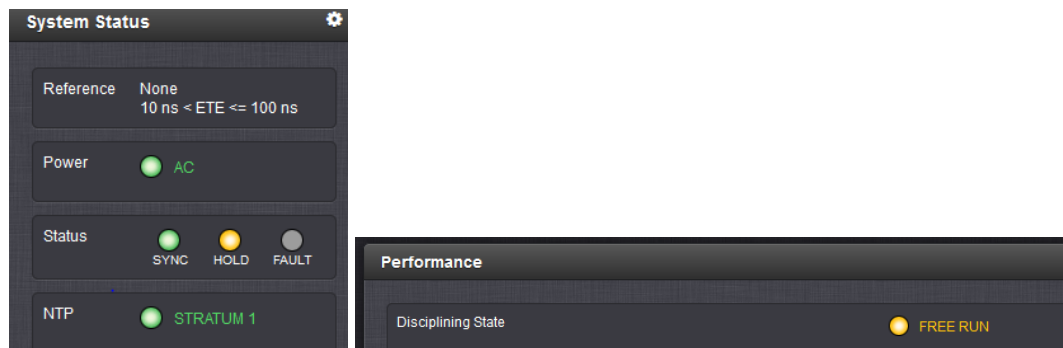
**“1PPS not in Specification” / “1PPS Restored to Specification” entries in logs**

These are events that occur and alarm entries that are asserted. “1PPS not in Specification” occurs if the current TFOM values exceed the user-configurable max TFOM value. When the TFOM falls below Max TFOM, the Restored to Specification event/alarm entry is asserted.

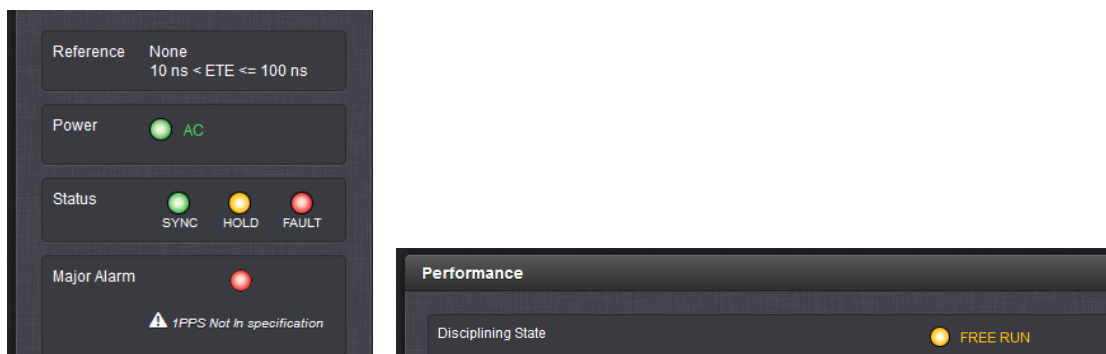
Regarding the “1PPS Not in Specification” alarm/trap, this alarm only occurs if the current TFOM exceeds the user-configurable max TFOM value. The SecureSync going into Holdover mode will not initially and automatically cause the TFOM to increase and exceed the max TFOM value. However, if the unit continues to operate for an extended period of time without any valid input references, the oscillator will begin to drift. As long as the max TFOM is not set to 15, eventually, the max TFOM will be exceeded and the alarm is asserted. The type of oscillator (OCXO or Rubidium) and the setting of max TFOM will determine the typical amount of time in holdover required to exceed the max TFOM.

**If SecureSync is already in Holdover mode, when TFOM starts to exceed MaxTFOM (due to estimated osc drift)  
Holdover mode (Holdover indicator is already yellow)**

- A) RB oscillator. No valid input references. MaxTFOM set to default “15”. TFOM is 2 (TFOM 2 not exceeding MaxTFOM 15)**



- B) RB oscillator. MaxTFOM changed to “1”. TFOM is 2 (TFOM 2 is now exceeding MaxTFOM 1)**



---

## Outputs

### \*\*OPT-TKL (Timekeeper software in SecureSync)

**Notice:** (As of at least Dec, 17) Timekeeper option is not compatible with the newer variant ETX module. I don't anticipate it will ever be compatible.

#### Customer service SecureSyncs with timekeeper license installed

(22 Aug 2018 KW) currently none- Morgan and I removed the license.

**Removal of Broadshield and Timekeeper software from existing 5.8.4/5.8.5 (and future) SecureSync upgrade bundles (for both Options to be removed from units, when the bundles are obtained from us after 10 Sept 2019)**

- Refer to ECO-FAI-2269 (in Arena): [https://app.bom.com/changes/detail-summary?change\\_id=2397735912&](https://app.bom.com/changes/detail-summary?change_id=2397735912&)
  - Title of ECO: “SecureSync 5.8.4 / 5.8.5 - Remove Timekeeper/Broadshield from software”
  - Effective date: 10 Sept 2019

### (Purchased Option for PTP/NTP functionality)

#### General Info

- Timekeeper software started being installed in SecureSync with the version 5.2.0 software update (Jan 2015)
- Refer to SecureSync user manual, rev 17 or higher (Section 4.5.1) for more info (Rev 21 is section 3.4)
- Two license files available for purchase (Timekeeper is providing two different functions)
  - PTPv1 support for a particular customer
  - Enhanced NTP/PTP monitoring capabilities and PTPv1/v2

---

### Timekeeper software on SecureSync not compatible on 64 bit linux (v5.7.0 and above)

- Version 5.7.0 - [refer to JIRA ticket SSS-279] – “Timekeeper will not run on a x64 unit”
- Refer to ECO-ITEM-001270

Email from Pierre (17 Oct 17) Eric G changed the ETX card on a SecureSync running with the TKL option. After two reboots, the SecureSync was running again but the TimeKeeper option is not running at all. The option is activated but it is not possible to start the process in the GUI.



Nothing happens when the service is started and each time I come back to the page the service is off. Are you aware of this issue, please?

### Way to tell from a saved config bundle whether timekeeper is enabled/being used on a SecureSync

**Per Ron D (23 Aug 2018) look in the /etc/runlevels/default directory to see if timekeeper is listed**

This PC > Spectracom (D:) > Spectracom > customer logs > PDT Partners > 172216 > etc > runlevels > default

| Name                              | Date modified      | Type      | Size |
|-----------------------------------|--------------------|-----------|------|
| <input type="checkbox"/> cagpsd   | 8/23/2018 11:42 AM | File      | 0    |
| <input type="checkbox"/> net.eth0 | 8/23/2018 11:42 AM | ETH0 File | 0    |
| <input type="checkbox"/> net.eth2 | 8/23/2018 11:42 AM | ETH2 File | 0    |
| <input type="checkbox"/> ntp      | 8/23/2018 11:42 AM | File      | 0    |
| <input type="checkbox"/> snmpd    | 8/23/2018 11:42 AM | File      | 0    |
| <input type="checkbox"/> snmpsd   | 8/23/2018 11:42 AM | File      | 0    |
| <input type="checkbox"/> sql_db   | 8/23/2018 11:42 AM | File      | 0    |

## IPv6 support with PTP

(2 Aug 17, KW) As of at least SecureSync version 5.7.0 (and timekeeper version 7.2.9), the SecureSync is not able to support IPv6 for PTP functionality (via the Option Cards or via the Timekeeper option). The 1204-12 and 1204-32 cards don't support IPv6, and timekeeper for SecureSync program does not currently support IPv6 with PTP, either.

**Per Dave Sohn (1 Aug 17)** unfortunately, there is no current IPv6 support for PTP on SecureSync.

**Per Dave Sohn (2 Aug 17)** I'm confused as to how this would be a defect ticket, but certainly we'll add it as a feature request. VelaSync does not support IPv6 for PTP either.

## Rubidium oscillator disciplining in a SecureSync with Timekeeper software installed

- Timekeeper software cannot discipline a Rubidium oscillator while its 1PPS source (PPS input) is NTP

**Email from Dave Lorah (20 Dec 16)** I have verified with Engineering support that the Rubidium Oscillator will not discipline if the Securesync is using an NTP Input. This is the same whether you use Timekeeper or not. I am sorry for the confusion.

The only way to discipline the oscillator on these Stratum 2 units is to use a 1PPS Input or another stable high quality reference. The NTP simply is not stable enough to discipline the Rubidium.

**Note:** When Time server is enabled/running, this license completely replaces the NTPv4 software that is normally installed with Timekeeper software. So web browser configuration fields for NTP are not the same as normal.

### From Section 4.6 of the SecureSync manual

#### What can TimeKeeper do for me?

TimeKeeper supports NTP, and IEEE 1588 PTPv1/v2. A user interface integrated into the SecureSync Web UI allows for enhanced status and timing quality monitoring, as well as a map of the timing network, displaying all the time sources detected.

If your SecureSync has a valid synchronization reference, TimeKeeper will operate as a Stratum 1 server, using SecureSync's system time. No configuration is required for NTP. One or more instances of a PTP master can be configured.

In the event SecureSync loses its synchronization to a high-quality reference, TimeKeeper will continue to act as a time server/master during the Holdover period plus 180 seconds, and then look to synchronize for a suitable reference source on its network, qualifying one of the configured NTP servers or PTP masters to become the system's reference, if network time ("NTP") is configured accordingly in the reference priority table.

TimeKeeper does not require additional hardware, i.e. option cards, because it can operate using the built-in 10/100 Mb network interface. If installed, however, TimeKeeper will utilize the additional 10/100/1000 ports offered by the 1204-06 multi-port option card (ETH1 and ETH2 can be used for hardware time stamping). Any of these ports can be configured for multiple PTP masters and slaves, and NTP sources, simultaneously.

## After purchasing license file

### Step 1: install/activate purchased timekeeper license file

- For instructions on installing a license file, refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\License Files Updates
- License files are purchased/generated for a specific Serial Number. It can only activate this option on the specified Serial Number.
  - Installed license files are displayed in the Tools -> Upgrade/Backup page of the browser
    - An additional “**Monitoring**” button will be displayed in top-right of the browser, once timekeeper license has been installed



If you do not see the Monitoring tab on the upper right corner of the SecureSync you need to install a license file to enable it. Please see the attached document on how to install a license file if needed. Please note each license file is custom and only works on one particular SecureSync Serial number.

## Step 2: enable Timekeeper software

- Timekeeper can be enabled in one of either two ways (refer to either A or B below):

**Note:** Timekeeper cannot be enabled via the **Management -> NTP Setup** page

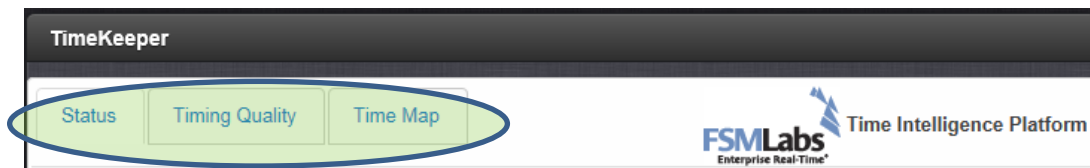
- A) Via the **Monitoring** page of the web browser (via the Timekeeper slider switch on the left)



- B) Via the Management -> PTP Setup page of the browser (via the PTP slider switch on the left)



Three tabs (Status, Timing Quality and Time Map) should now be displayed towards the top of the Monitoring page



If the three Timekeeper tabs aren't visible at top of “Timekeeper Monitoring” page

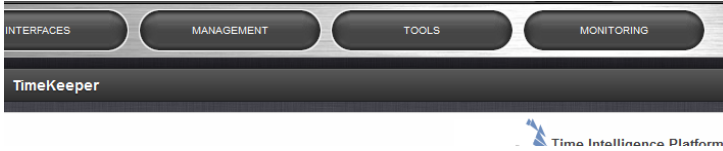
1. Need to be logged in with “HTTPS” (not HTTP)

**Important Note:** Monitoring Requires HTTPS (Secure) connection with the SecureSync's web browser!!

**Otherwise, the screen will look like:**



## 2. Timekeeper tabs aren't visible at top of "Timekeeper Monitoring" page with **Firefox** browser



- Looks like you need to use Internet Explorer or Chrome (not Firefox)



---

### \*\*\*Timekeeper software operation

**Note:** Refer also to the Velasync section of the VelaSync/Geo Tech note for additional info on operation of Timekeeper (in addition to the following info): <I:\Customer Service\1- Cust Assist documents\VelaSyncAndGeoCustAssist.pdf>

---

#### Network port associated w/Timekeeper being activated (port 8888)

- Port **8888** is for the Timekeeper GUI interface

**Email from Ron Dries to Pierre (8 Sept 17)** "TimeKeeper runs on port 8888. When TimeKeeper is enabled in SecureSync port 8888 will be open and in use."

#### Potential vulnerabilities reported on port 8888 (Timekeeper software)

- Can use IPTables to close this port (see info below in blue)
- Refer to Salesforce case 117611

**Email from Ron Dries to Pierre (8 Sept 17)** "FSM runs their own webserver for TimeKeeper on port 8888. We do not control this webserver. The only control we have to close these vulnerabilities is to not run TimeKeeper."

**Email from Ron D to Pierre (27 Oct 17)** Does the customer need the TimeKeeper UI to be displayed?

Port 8888 is only used to display the TimeKeeper UI in the SecureSync web UI.

We can provide a command which will block port 8888 and resolve the security scan findings.

No configuration is done through the TimeKeeper UI it only displays status. Most of this status information can be found in other web pages or from the command line.

The customer checked with his colleagues, and they need to use TimeKeeper to check their PTP networks. However, they found that there is a non-compliance regarding the PCI rules related to the port 8888. I assume that your solution will keep TimeKeeper running but blocked the access into the Web UI of the SecureSync. If so, how can they check the PTP status and get the benefit of TimeKeeper, please? Is it possible to have some CLI commands instead

**F/U email / Fix from Dave Sohn to Pierre (27 oct 17)** From the command line you can utilize the iptables command from an admin account like spadmin. This will block all incoming traffic to port 8888. Ron Deies can correct any information, if necessary.

```
sudo iptables -I INPUT -p tcp -dport 8888 -j DROP
```

---

#### Possible need to disable SecureSync's host discipling (when using NTP input with timekeeper software)

##### Intermittent Holdover or continuous loss of sync when tinmekeeper is syncing via NTP servser

Email from Dave L to Engineering: "I ran a duplicate scenario to theirs overnight where a Securesync v5.4.5 running Timekeeper is syncing to time.nist.gov. Timekeeper is syncing just fine but I am seeing the Securesync go in and out of Holdover every few minutes. This will produce traps and email messages on their monitoring. Can anything be done to prevent this from going in and out of Holdover?"

- If Host Disciplining is enabled, NTP input (especially when syncing to an Internet Time server), will likely cause excessive jittering of the oscillator. This can adversely affect Timekeeper's sync/operation.
- Recommended to disable host disciplining when using tinmekeeper to sync to other NTP servers ([Management - > NTP Setup](#) page). Refer to (in this document): Host disciplining of oscillator when NTP or "User set time" is the selected reference

**Email from Ron (16 Nov 16)** They should check if host disciplining is enabled, and if so, disable it. It won't work well with an open internet source like that and may be the source of the issue.





2. Click the **+** icon in the upper-right corner of “PTP Masters to add a new PTP Master

#### Field descriptions

- **PTP Server Version:** Ver.1 or Ver.2 (PTPv1 or PTPv2)
- **Note about issue with PTPv1:** There is a timekeeper software issue with PTPv1 in timekeeper versions prior to v7.11 (this will be the case in all SecureSync software versions to at least 5.4.5, if not higher)

**Issue report from a demo SecureSync customer:** I loaded the latest license file. Now, the PTP option is on. I configured the PTP with version 1, and I can capture the PTPv1 time message out of Ethernet ETH1 port. However, the Sync message was not compatible with the PTP time message format. The UDP payload (Length) should be 132 instead of 136. The GrandmasterPreferred byte should be on byte 77<sup>th</sup> of UDP payload, not byte 76<sup>th</sup>.

**Email from Matt Sherer (9 Nov 16) Confirming with that version here, that was an issue in 7.0.6, but got resolved. The fix is in the TimeKeeper 7.1.1 release we made for the SecureSync - so if you can update the customer to use that version they should be all set. I don't know how that integrates to the SecureSync packages, but maybe Denis has some ideas there about getting an integrated build with the 7.1.1 release?**

- **PTP Domain:** Determines which domain the PTP server will broadcast on. [Range 0-255] Default suggested domain for PTP1: 0.
- **PTP Server Sync Rate:** The rate at which to broadcast PTP synchronization messages (in seconds).
- **EXAMPLE:** “1” will cause SecureSync to broadcast a synchronization message every second, whereas “2” will send out messages in 0.5-second intervals. [Range: 0.5-64] Suggested setting:
- **PTP Server TTL:** This numeric field determines how long a PTP packet will live, in seconds, when routed (“Time-To-Live”) Suggested setting: 1 s
- **PTP Priority 1 [2]** The value set in these two fields will be broadcast by the PTP Master with announcement messages [Range: 0-255] Suggested setting: 128
- **Interface:** The name of the interface for PTP data this PTP Master will use. The interface name must correspond with a Linux network device name. Depending on the configuration of your unit, you can select any of the ports listed in this field.
- **Note:** Ensure that the selected interface is enabled: Go to MANAGEMENT Network , and click on the GEAR icon next to the port you want to use. Enable and configure the port in the Edit Ethernet Port Settings window.
- **Always Unicast Delay Responses** Check this box if you would like the PTP Master to provide unicast delay responses, no matter if the client provided a unicast or a multicast delay request. When the box is unchecked, the server will respond with the same type of message as the request:
  - a multicast response for a multicast request
  - a unicast response for a unicast request.
  - Recommended setting: Unchecked

3. Click **Submit**, and wait for the screen to refresh (TimeKeeper will be restarted)

#### Note about delay mechanism (P2P versus E2E)

As of at least Apr, 2016, **E2E** (End to End) is the **only** supported mode for the Timekeeper software. Denis Reilly does not believe that any Timekeeper software, including this available option, supports P2P mode (Peer to Peer).

- As of at least Apr, 2016, the Model 1204-12 10/100 PTP card is the only available PTP product which supports peer to peer. The 1204-32 does not support it either and I'm not aware of any plans for it to be added to this product (it only supports the telecom profile- not the power profile which uses P2P).

## PTP Slaves (PTP sources/PTP input)

### Step 4: Optionally Add PTP Slaves (Timekeeper “Sources” to sync the SecureSync to one or more PTP Masters)

PTP Slaves are used in a network to listen for synchronization packets from PTP Masters, and send out synchronization requests, as well as follow ups. The timing information from PTP masters are used by the system as a synchronization source if NTP is an entry in the reference priority table (it is by default), and no other reference set as a higher priority is available for synchronization. No configuration is required other than setting up PTP Slaves

1. **Management** -> **PTP Setup** page.



2. Click the + icon in the upper-right corner of PTP Slaves to add a new Slave

#### Field descriptions

- **NTP Client Version:** Version 1 or Version 2
- **PTP Server:** The address of the PTP server (this field will be populated by TimeKeeper, if only one server has been configured).
- **PTP Domain:** Determines which domain the PTP server will broadcast on. [Range: 0-255; default-suggested domain for PTP1: 0]
- **Low Quality Source:** Check this box to improve tracking of low quality sources, such as NTPd. [Default: Checked]
- **Unicast Delay Requests:** Enables unicast delay requests back to the server. Check this box if you would like the PTP Master to provide unicast delay responses, no matter if the client provided a unicast or a multicast delay request. When the box is unchecked, the server will respond with the same type of message as the request, that is a multicast response for a multicast request, and a unicast response for a unicast request. [Recommended setting: Unchecked]
- **Use Transparent Clock Corrections:** Check to allow the slave to apply the transparent clock correction provided with PTP data. [Default: Checked]
- **Permit Lost but Promised Followups:** Check this box to allow missing followup messages to handle certain network issues.
- **Unchecked [default]:** A PTP grandmaster that promises a followup message must deliver one in order for this slave to use a given time update. (This setting is recommended, since missing followups are a good

indication of an issue with PTP delivery or the grandmaster.)

**Checked:** A failed followup delivery will not prevent a time update updated.

- **Interface:** The name of the interface for PTP data this PTP Slave will use. The interface name must correspond with a Linux network device name. Depending on the configuration of your unit, you can select any of the ports listed in this field.
- **Note:** Ensure that the selected interface is enabled: Go to MANAGEMENT> Network and click on the GEAR icon next to the port you want to use. Enable and configure the port in the Edit Ethernet Port Settings window

3. Click Submit, and wait for the screen to refresh

## NTP input (NTP sources)

### Step 5: Optionally add one or more NTP servers that the SecureSync can sync with (via eth0, eth1, eth2 or eth3)

Similar to the concept of PTP masters as an external reference, TimeKeeper allows external NTP servers to be used by the system as a synchronization source if NTP is an entry in the reference priority table (it is by default), and no other reference set as a higher priority is available for synchronization. No configuration is required other than setting up NTP Source

#### Adding a new NTP Source

1. **Management** -> **NTP Setup** page.
2. Click the **Gear** icon in the upper-right corner to the right of “NTP Servers” and just below the “**Monitoring**” button)
3. Click the “+” in the upper-right corner In the “**NTP Servers**” pop-up window that opens



#### Field descriptions

- **NTP Server:** The IP address or DNS name of the NTP server to sync to
  - **NTP Sync Rate:** the rate at which to make NTP requests to the configured NTP
  - **Note:** a sync rate of 0.5 causes timekeeper to query the configured NTP server every 2 seconds
- Q Is there a default value for the NTP SYNC RATE? What is the recommended setting for this. We set it to 0.9 as in the example.
- A. Reply from Dave Loran (13 Jul 16) The default NTP behavior is recommended which is to leave that number blank. TimeKeeper will manage best it's sync rate with the NTP server and will obey its rate requests as required. Overriding this is not usually beneficial.
- **Low Quality Source:** Check this box to improve tracking of a low-quality source, such as NTPd.
  - **DNS Re-Resolve:** if checked, the source will periodically re-resolve the DNS name specified for the NTP source.

**Symmetric Key authentication:** MD5 authentication was not available in Timekeeper software versions prior to v7.2.0 (such as earlier version 7.0.6 installed in the first release of Timekeeper inside SecureSync. This function of NTP is not available in SecureSync as of at least Nov, 2016).

---

### \*\*\* Timekeeper NTP outputs/PTP outputs

#### E) PTP outputs

##### Hardware timestamping (using timekeeper software) versus software timestamping

- Hardware timestamping provides much greater accuracy than software timestamping.
- Hardware timestamping is only available on the three Gb Ethernet ports (1204-06 card)
- Eth0 only supports software timestamping. It should not be used for greater accuracies with the timekeeper PTP/NTP outputs (timekeeper doesn't use eth0). Typical NTP accuracies of 1 to 10 ms applies.

##### From the SecureSync manual:

TimeKeeper does not require additional hardware, i.e. option cards, because it can operate using the built-in 10/100 Mb network interface. If installed, however, TimeKeeper will utilize the 3 additional 10/100/1000 ports offered by the 1204-06 multi-port option card (ETH1 ETH2 and Eth3 can be used for hardware time stamping). Any of these ports can be configured for multiple PTP masters and slaves, and NTP sources, simultaneously.

##### List of PTP clients being serviced by the VelaSync/Timekeeper

| Current Client Snapshot Details |        |                  |               |                          |
|---------------------------------|--------|------------------|---------------|--------------------------|
| Client                          | Source | Estimated offset | One way delay | Age of update in seconds |
| 10.10.128.14                    | 0      | 0.010330358      | 0.000350958   | 7                        |

Q. For the PTP protocol in both VelaSync and SecureSync, is there a mechanism to see how many client/machine are connected to the grandmaster.

A. Yes, you do but they are very different from one another. On the SS, it gives a summary count of the unicast slaves and you can get more detail by clicking on the (i) button next to it. On the VelaSync we have what is called a "Time Map", which gives a graphic representation of the network.

---

#### F) NTP outputs

##### Hardware timestamping (using timekeeper software) versus software timestamping

- As long as Timekeeper is enabled, shouldn't have to do anything else for the SecureSync to be an NTP server.
- Hardware timestamping provides much greater accuracy than software timestamping.
- Hardware timestamping is only available on the three Gb Ethernet ports (1204-06 card)
- Eth0 only supports software timestamping. It should not be used for greater accuracies with the timekeeper PTP/NTP outputs (timekeeper doesn't use eth0). Typical NTP accuracies of 1 to 10 ms applies.

##### From the SecureSync manual

TimeKeeper does not require additional hardware, i.e. option cards, because it can operate using the built-in 10/100 Mb network interface. If installed, however, TimeKeeper will utilize the 3 additional 10/100/1000 ports offered by the 1204-06 multi-port option card (ETH1 ETH2 and Eth3 can be used for hardware time stamping). Any of these ports can be configured for multiple PTP masters and slaves, and NTP sources, simultaneously.

### **\*\*\*NTP Client lists (timekeeper's TimeMap function VS the NTP Client List in standard NTP)**

#### **A) Timekeeper software not enabled**

- Refer to [View NTP Clients](#) (in the NTP section of this document) for more info on the NTP Client List for NTPD
- Button for the NTP client table is on the left-side of the *Management* -> *NTP Setup* page of the browser.

#### **B) If Timekeeper software is enabled (purchased license file required)**

- If timekeeper software is enabled, it replaces NTPD. So the normal NTP Client list for NTPD (mentioned above) is not available.
- Timekeeper software provides a "TimeMap" function for reporting which NTP (and PTP) clients it can see on the network.

If Timekeeper is enabled, it can report all of the PTP Clients it sees on Ethernet ports eth0-eth3 (if PTP Option Cards (such 1204-12 and/or 1204-32 are also installed in the SecureSync, Timekeeper can't report any PTP clients that may be isolated to the PTP Option Cards.

## \*\*\*Timekeeper configs / Timekeeper logs

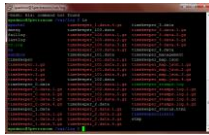
### A) Timekeeper.conf file (timekeeper configs)

- Stored in **/etc** folder
- Refer to the VelaSync tech note for additional info.
- Per Ron and Paul, Timekeeper configs are retained in the standard SecureSync log bundle.
  - Example timekeeper.conf file



### B) Timekeeper.log and other timekeeper log files

- **Displayed: Tools -> Timekeeper** page of the SecureSync's browser
- Timekeeper log entries are in the SecureSync's **daemon** log
- Timekeeper log entries are stored in SecureSync's var/log directory:



- Refer to the VelaSync tech note for additional info on the various timekeeper logs.

### GPS-associated log entries (source 0): timekeeper\_0.data file

```
admin@spectracom /var/log $ cat timekeeper_0.data
979930212.288600218 0.000000472 -0.000000985 218100201199988 -0.000090119 0.000000000 0.000000000 0.000000058
s00,AntoPEN,satview32,satuse09,sigmax55dBHz,sigavg13dBHz 0.000009103 0.000012506 spectracom -0.000090116 0.0
00959 0.000000000
admin@spectracom /var/log $
```

### Logs for the NTP/PTP clients syncing via timekeeper software: cd timekeeperclients

```
admin@spectracom /var/log/timekeeperclients $ ls
10.2.100.171_0_data 10.2.100.220_0_data-1.01 10.2.100.92_0_data-1.01 10.2.100.0-1_0_data
10.2.100.171_0_data-1.01 10.2.100.220_0_data-2.01 10.2.100.92_0_data-1.01 10.2.100.0-1_0_data-1.01
10.2.100.171_0_data-2.01 10.2.100.60_0_data 10.2.100.92_0_data-1.01 10.2.100.0-1_0_data-1.01
10.2.100.171_0_data-3.01 10.2.100.60_0_data-1.01 10.2.100.92_0_data-2.01 10.2.100.0-1_0_data-1.01
10.2.100.240_0_data-1.01 10.2.100.60_0_data-2.01 10.2.100.92_0_data-3.01 10.2.100.0-1_0_data-1.01
10.2.100.240_0_data 10.2.100.60_0_data-3.01 10.2.100.92_0_data-4.01
admin@spectracom /var/log/timekeeperclients $
```



### \*\*\*Timekeeper Status Monitoring of NTP/PTP Clients and servers

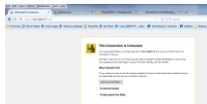
**Important Note:** Monitoring Requires HTTPS (Secure) connection with the SecureSync's web browser!!

Otherwise, the screen will look like:

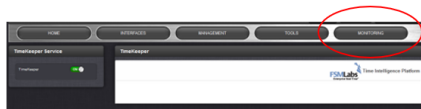


Status Monitoring needs to first be enabled in the browser in order to be available

- Login to Timekeeper using HTTPS 0In the URL address line, add “**https://**” to the front of the SecureSync's IP address



- Click on **Monitoring** on top-right corner

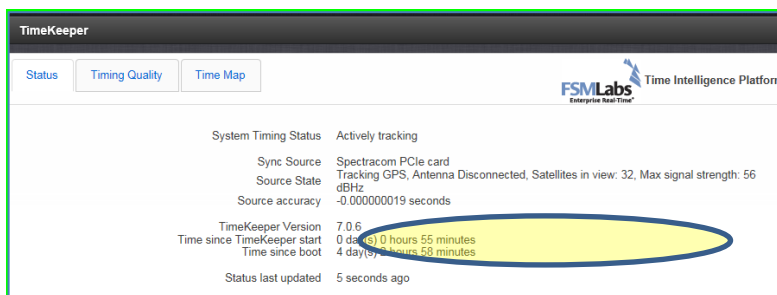


Once the status monitoring functionality has been enabled, it can be accessed via the **MONITORING** button in the **Main Navigation bar**.

The TimeKeeper monitoring interface has three tabs:

#### A) “**Status**” tab

- The Status tab provides information on the source currently tracked, as well as TimeKeeper system data, and system tracking information
- Similar to, but not identical to timekeeper in VelaSync:



#### Sync Source field

- Will indicate Spectracom PCI Card, NTP or PTP, depending on the selected Source
- “Spectracom PCI Card”: indicates Timekeeper software is synced via Source 0 (GPS/GNSS, via the TSync driver)
- If it indicates “NTP” or “PTP” input (instead of Spectracom PCI Card”, Source 0 (GNSS/GPS) is not currently the selected reference. This means either:
- The GNSS receiver is not currently tracking any satellites (GNSS 0 is not a valid input) OR
- **The GNSS 0/GNSS 0** reference is not listed and enabled in the **Management-> Reference Priority** page of the

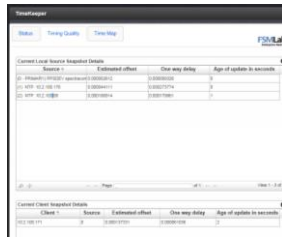
browser.

### Source state field

- “Antenna disconnected:” indicates either there is no GPS/GNSS antenna connected, or the antenna sense circuit in the receiver is detecting an open/short in the cable (such as GPS splitter being installed inline) even though the cabling is fine.

### B) “Timing Quality” tab

- The Timing Quality tab offers detailed information on the quality of NTP and PTP sources, such as timing offsets and delays.



| Source ID         | Estimated offset | One-way delay | Age of update to seconds |
|-------------------|------------------|---------------|--------------------------|
| 00:00:00:00:00:00 | 0.000000         | 0.000000      | 0                        |
| 00:00:00:00:00:00 | 0.000000         | 0.000000      | 0                        |
| 00:00:00:00:00:00 | 0.000000         | 0.000000      | 0                        |

| Client ID         | Source   | Estimated offset | One-way delay | Age of update to seconds |
|-------------------|----------|------------------|---------------|--------------------------|
| 00:00:00:00:00:00 | 0.000000 | 0.000000         | 0             |                          |
| 00:00:00:00:00:00 | 0.000000 | 0.000000         | 0             |                          |
| 00:00:00:00:00:00 | 0.000000 | 0.000000         | 0             |                          |

### C) “Time Map” tab

- Under the Time Map tab, TimeKeeper TKL visualizes the structure of the timing network environment, including all time sources and other clients found on the network. Especially with complex networks, this visualization tool can be of assistance when it comes to identifying architectural or accuracy problems



### PTP Client lists (to report number and which PTP clients are being serviced)

- Refer to the PTP -> General info Section of the SecureSync Option Card document.

### Timekeeper NTP operational info (timekeeper enabled)

- Refer to the VelaSync assistance doc for more info on Timekeeper NTP configuration/operation
- NTPD is disabled (“removed”) when Timekeeper is enabled. NTP is handled by timekeeper

### D) List of NTP clients If Timekeeper software is enabled (purchased license file required)

- If timekeeper software is enabled, it replaces NTPD. So the normal NTP Client list for NTPD (mentioned above) is not available.
- Timekeeper software provides a “TimeMap” function for reporting which NTP (and PTP) clients it can see on the network.

If Timekeeper is enabled, it can report all of the PTP Clients it sees on Ethernet ports eth0-eth3 (if PTP Option Cards (such as 1204-12 and/or 1204-32 are also installed in the SecureSync, Timekeeper can't report any PTP clients that may be isolated to the PTP Option Cards.

## List of PTP clients being serviced by the VelaSync/Timekeeper

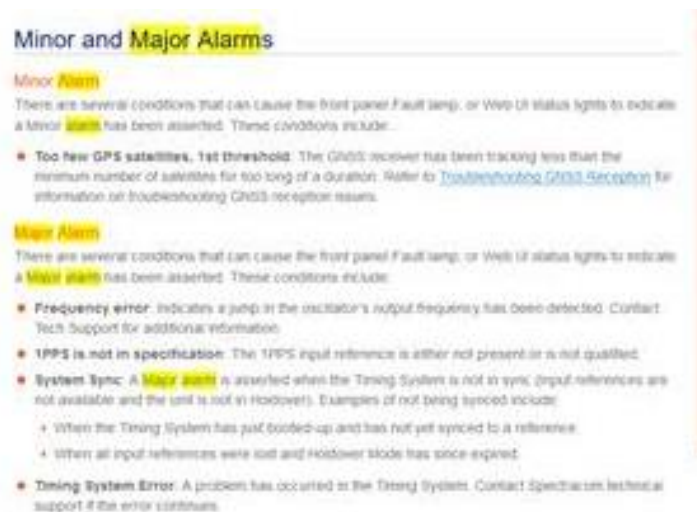
| Current Client Snapshot Details |        |                  |               |                          |
|---------------------------------|--------|------------------|---------------|--------------------------|
| Client                          | Source | Estimated offset | One way delay | Age of update in seconds |
| 10.10.128.14                    | 0      | 0.010330358      | 0.000350958   | 7                        |

- Q. For the PTP protocol in both VelaSync and SecureSync, is there a mechanism to see how many client/machine are connected to the grandmaster.
- A. Yes, you do but they are very different from one another. On the SS, it gives a summary count of the unicast slaves and you can get more detail by clicking on the (i) button next to it. On the VelaSync we have what is called a "Time Map", which gives a graphic representation of the network.

---

## System Alarms (Major and Minor alarms)

- Refer to the online SecureSync user guide for Minor and Major alarms [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TROUBLE/MinMajAlarm.htm?Highlight=major%20alarm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TROUBLE/MinMajAlarm.htm?Highlight=major%20alarm)



### A) Alarms classified as Major alarms

#### 1. 1PPS is not in specification

- The 1PPS input reference is either not present or is not qualified. TFOM exceeds Maximum TFOM (MaxTFOM)

---

#### 2. (User-defined Major alarm) (GPS receiver)

This alarm indicates a user has configured the NTP time server to assert a Major alarm upon the GPS receiver falling below a specified number of satellites, for a user-specified length of time. For example, a user can configure this alarm to be asserted if the unit was tracking at least five satellites, but sometime thereafter, it starts tracking only three satellites, by setting the threshold at 4 satellites. Since this alarm threshold is not directly related to the minimum number of satellites required by the system, the presence of this alarm does not automatically indicate a problem with GPS reception.

The number of satellites for the alarm threshold and whether the receiver dropping below this user-specified number of satellites is classified as a Major alarm or as a Minor alarm is configured in the System/Alarm page of the web browser.

---

#### 3. GPS receiver fault

- indicates a problem with the internal GPS receiver.

---

#### 4. Time Sync alarm

- Indicates the NTP server has lost synchronization to its external reference (GPS, IRIG etc) and has also timed-out of the Holdover mode (as configured in the System/Holdover page of the browser) OR The unit was rebooted (it will be in a Time Sync alarm until it is resynced to its external reference after every reboot/power cycle).
  - **Note:** this alarm is asserted after every boot-up

---

## 5. Rubidium Monitor alarm:

- Indicates a potential issue with the Rubidium oscillator has occurred.

**Note:** This alarm can be caused by a low voltage input to the NTP time server. Time servers with Option 4 installed require 24vdc input power instead of 12vdc input. If the time server has 12vdc applied, the time server may appear to be operating normally with this alarm present.

During the Time Sync Alarm, all of the outputs, including NTP, will indicate that the NTP server is not in sync. In most cases, PCs and other systems connected to the NTP server will ignore it while the Time Sync alarm is present. They will likely fall back to using their own internal time base to derive the time. The primary external reference will need to be restored for devices to be able to use the NTP server as a time reference (or it may need several minutes to resync to the primary reference if it was recently rebooted/power cycled).

---

## 6. Frequency error alarm (Freq Error alarm):

**Note:** this alarm is asserted after every boot-up

- Frequency Error alarm is NOT due to the size of the frequency error. It means the DAC is within 10% of its max range

**Per Dave Sohn (2 Dec 2020)** The frequency alarm is related to the DAC as a frequency control alarm that is set if we get within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values.

**Email Dave L sent (8 Dec 2020)** The jump in the oscillator frequency may not trigger a Frequency Alarm.

In the Securesync, the frequency alarm is generated when the DAC which controls the oscillator frequency gets within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values shown in the oscillator log.

To trigger an alarm if the phase error exceeds a certain threshold, the user could set a "Max TFOM for Sync" value which will automatically switch the Securesync to Holdover mode if a certain phase error values is exceeded. The Holdover event will trigger alarms from the Securesync.

Here is the section of the User Manual with more information:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/OscConfiguring.htm?](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm?)

**The Frequency Error Alarm is asserted when 10 MHz Frequency Error measurement exceeds a set threshold (oscillator dependent)**

- **TCXO oscillator:**  $1 \times 10^{-7}$  in v5.3.0 and below (changed to  $1 \times 10^{-6}$  starting in v5.3.1 to address. See note below about Mantis case 3168)
- **OCXO oscillator:**  $1 \times 10^{-8}$
- **Rubidium (and low phase noise Rubidium-LPN Rb):**  $1 \times 10^{-9}$

**Note:** (Applicable only to the Hughes special CGU SecureSync) the Frequency Error Alarm can also be asserted due to PLL Lock issues associated with the Wentzel oscillator. Refer to the Specials section of this doc for more info on this special.

### **Mantis case 3168: Issue with TCXO oscillator asserting Freq Error Alarms when exiting Sync**

- Issue with software versions 5.3.0 and below (fixed in version 5.3.1, Dec 2015)
- Refer to Mantis case 3168 (Freq error threshold needed to be changed to  $1 \times 10^{-6}$  instead of  $1 \times 10^{-7}$ )

**Determine type of oscillator installed:**

- A) Via newer Web browser: *Management* -> *Disciplining* page

B) Via CLI command: `XO_GetOsctype` <enter>

### Possible causes of the Freq Error alarm (Frequency Error alarm) being asserted

**Email from Dave Sohn (5 Dec 2020)** The frequency alarm is related to the DAC as a frequency control alarm that is set if we get within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values.

**Per Dave Sohn:** The Frequency Error Alarm should only ever be asserted if a disciplining reference (such as GPS) is present/valid (and also at boot-up). However, there have been a couple of software issues causing it to be asserted when it shouldn't be.

#### 1. Measured Frequency error exceeds:

- **Rubidium (and low phase noise Rubidium-LPN Rb):** Measured frequency error exceeds  $1 \times 10^{-9}$
- **OCXO oscillator:** Measured frequency error exceeds  $1 \times 10^{-8}$
- **TCXO oscillator:** Measured frequency error exceeds:
  - $1 \times 10^{-7}$  in v5.3.0 and below
  - $1 \times 10^{-6}$  starting in v5.3.1 to address.

### Mantis cases associated with Frequency Error Alarms

#### 1. Mantis Case 3168 (TCXOs)

- Versions 5.3.0 and below for TCXO
  - Software condition in v5.3.0 (and possibly earlier) causing sporadic Freq Error alarms to be asserted when exiting full sync (going into Holdover mode)
  - Refer to Mantis case 3168
  - Caused by the TCXO Frequency error threshold being too tight (currently  $1 \times 10^{-7}$ . but needs to be decreased to  $1 \times 10^{-6}$  instead)
  - In at least software version 5.3.0 (addressed in update version 5.3.2, Dec 2015)

#### 2. Mantis case 3166 (TCXOs and OCXOs)

- Versions 5.3.0 and below for TCXO or OCXO oscillator installed
  - **TCXO and OCXO oscillators** Software condition in v5.3.0 (and possibly earlier) causing sporadic Freq Error alarms to be asserted
  - Refer to Mantis case 3166
  - Refer to salesforce case 19701 (for Esther Shieh)
  - Associated with the osc disciplining algorithm causing large osc shifts
  - Version 5.3.1 made several improvements to the oscillator disciplining of TCXO/OCXO and Low Phase Noise Rubidium
  -

#### 3. Other reasons the Freq Error alarm may be asserted

- A Wenzel oscillator is installed in / connected to the SecureSync (such as with the "CGU SecureSync" special for Hughes) and there is an issue with either of the two (2) PLL circuits in the Wenzel oscillator
- Note: Associated lock status messages are asserted in the oscillator log (refer to osc.log or CGU for Hughes in this document for details)

- This alarm is asserted after each boot-up for a period of time (it should clear within a few minutes later- its asserted until the oscillator has been coarse adjusted.)
- Jitter on the input reference (such as PTP IRIG or external 1PPS input, for example).
- Switching from one reference to another.
- Enabling at least one reference in the Reference Priority table (with all references previously disabled)
- Performing a restart tracking of the oscillator.
- Faulty oscillator
- TCXO oscillator with versions
- Syncing via NTP input with either:
  - Rb oscillator installed OR
  - Software versions 5.3.0 and below with TCXO/OCXO installed (host disciplining for TCXO/OCXO was added in v5.3.1)

**Note: Freq Error alarm can be asserted when the Freq error is reported **AT** the threshold (not exceeded) due to “rounding”**

- There is rounding that goes on in the oscillator frequency errors in the logs. So if the log indicates a frequency count AT the specified threshold, the Frequency Error alarm can still be asserted, because the measured values in decimal values still exceeded the threshold (for example with a Rb oscillator- if the actual frequency error is 3.0000001, the osc.log entry may show it as 3.000 but the actual value still exceeds the threshold. So the Freq alarm was asserted.

### Clearing of the Freq Error (Frequency Error alarm)

- The Frequency Error Alarm clears when 10 MHz Frequency Error measurement is less than the set threshold

---

## B) Alarms classified as Minor alarms

### 1. In Holdover alarm (“In Holdover” mode event)

- Mantis case 3249: Note that in at least software versions 5.4.1 and below, Holdover is an **Event** (entry asserted in the **Events** log) instead of being an Alarm (not asserted as an entry in the Alarms log)

Indicates the NTP server lost synchronization to its external reference input and it’s using the internal reference oscillator to derive the time outputs. This alarm is classified as a Minor alarm condition. The Holdover mode will continue until the reference is restored, it times out as configured in the System/Holdover page, or the unit NTP server is rebooted/power cycled. If Holdover mode times out, at that time a Time Sync alarm will be asserted.

During the Holdover mode, all outputs remain available to synchronize other devices. This mode is just an alert that the primary input is not available and so the oscillator is being used to provide time outputs. There is no other effect on the operation of the system while in the mode.

#### “In Holdover” and “Not in Holdover” event entries are always masked in versions prior to version 5.4.4

- Prior to version 5.4.5, both of these events were listed in the Notifications page but the checkbox to mask/unmask them were not visible. And in the background, they were always selected (it was this way since we added the ability to mask alarms.
- Version 5.4.5 (~Aug 2016) is adding visible Holdover/Not in Holdover MASK checkboxes to the Management -> Reference Priority page (previously these were listed with no checkboxes available. The factory default settings are for these two checkboxes to be selected (Holdover alarms masked). But starting with Version 5.4.5,

customers can now unmask these alarms so that they are asserted, as desired.

---

## 2. User-defined Minor alarm (Min Sats):

This alarm indicates a user has configured the NTP time server to assert a Minor alarm upon the GPS receiver falling below a specified number of satellites, for a user-specified length of time. For example, a user can configure this alarm to be asserted if the unit was tracking at least five satellites, but sometime thereafter, it starts tracking only three satellites, by setting the threshold at 4 satellites. Since this alarm threshold is not directly related to the minimum number of satellites required by the system, the presence of this alarm does not automatically indicate a problem with GPS reception.

The number of satellites for the alarm threshold and whether the receiver dropping below this user-specified number of satellites is classified as a Major alarm or as a Minor alarm is configured in the:

- **Newer browser:** Management -> Notifications page of the browser, GPS tab
  - **classic interface web browser:** System -> Alarm page
- 

## 3. User-defined Minor Alarm (Temperature alerts) (Versions 5.3.1 and above only):

This alarm indicates a user has configured the NTP time server to assert a Minor alarm when the internal temperature has exceeded the min or max custom-configurable threshold (**Management** -> **Notifications** page of the browser, **System** tab):

### C) Newer browser: Management -> Notifications page of the browser, GPS tab

| Minor Alarm Threshold   |                          |
|-------------------------|--------------------------|
| Minimum Temperature (C) | Readings above Threshold |
| 100                     | 1                        |

| Major Alarm Threshold   |                          |
|-------------------------|--------------------------|
| Minimum Temperature (C) | Readings Above Threshold |
| 100                     | 1                        |

### D) Classic interface web browser:

- Not available in the classic interface browser (feature was added in version 5.3.1)
- 

## 4. Antenna Problem alarm:

This alarm log entry indicates an open or short has been detected by the GPS receiver in the antenna cable (Located somewhere between the NTP time server and the GPS antenna). This alarm is classified as a Minor alarm condition. If this alarm is present, refer to the "GPS Troubleshooting guide (<http://www.spectracomcorp.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=396&PortalId=0>) for troubleshooting assistance.

---

## 5. Oscillator Adjust:

Indicates a potential issue with the internal oscillator calibration.

---



**6. The unit has rebooted:**

SecureSync was either rebooted or intentionally/inadvertently power cycled.

## Desire to mask or unmask alarms/events

- Refer also to the SNMP tech note: I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP
- Ability to mask alarms was added in version 4.8.7

In some SecureSync configurations, there may be one or more alarm conditions that will remain always asserted, so the associated alarm(s) may need to remain active. This results in the front panel “Fault” LED remaining lit. Starting in Archive software version 4.8.7, undesired “Spectracom-specific” alarms can be “masked” (squelched) to prevent undesired alarms from being continuously asserted.

Log entries are still inserted for masked alarm conditions, but traps and emails aren’t sent for masked alarm conditions. And masking undesired alarm conditions can allow the front panel “Fault” LED to clear when all other “non-masked” alarm conditions have cleared.

Masking is configured in the **Management-> Notifications** page of the newer (black) web browser. There are various tabs for all of the available alarms/events which can be masked, as desired. (These events/alarms are listed and described in the SNMP Tech Note at the link further above).

**Factory default settings:** Most, but not all, alarms/events are not masked by default. Exceptions are the “**In Holdover**” and “**Not in Holdover**” events which are masked by factory default.

### “In Holdover” and “Not in Holdover” event entries are always masked in versions prior to version 5.4.4

- Prior to version 5.4.5, both of these events were listed in the Notifications page but the checkbox to mask/unmask them were not visible. And in the background, they were always selected (it was this way since we added the ability to mask alarms).
- **Version 5.4.5** (~Aug 2016) is adding visible Holdover/Not in Holdover MASK checkboxes to the **Management -> Reference Priority** page (previously these were listed with no checkboxes available. The factory default settings are for these two checkboxes to be selected (Holdover alarms masked). But starting with Version 5.4.5, customers can now unmask these alarms so that they are asserted, as desired.

---

## \*\*Obtaining Time/Date reads (desire to read/obtain time remotely/automatically)

- 1) Can view the **Setup -> Time Management** page of the browser
- 2) Can use the Models **1204-02** (RS-232) or **1204-04** (RS-485) Option Cards to automatically output ASCII time stamps (broadcast or interrogation modes).
- 3) Can read the time/date via CLI interfaces (front panel SERIAL port, telnet or ssh) using the following commands:

**Note:** CLI interfaces, including the front panel DB9 connector, are all username/password protected. Login is required to use CLI interfaces to obtain date/time stamps)

- **dateget** (displays current date)

```
spfactory@Spectracom ~/log/discstats $ dateget
03 JUL 2014
spfactory@Spectracom ~/log/discstats $
```

- **doyget** (displays current day of year)

```
spfactory@Spectracom ~/log/discstats $ doyget
184
spfactory@Spectracom ~/log/discstats $
```

- **timeget** (Displays the current System Time – the time scale of this reported time is based on the System Time scale which is configured in the **Setup -> Time Management** page of the browser)

```
spfactory@Spectracom ~/log/discstats $ timeget
13:50:39
spfactory@Spectracom ~/log/discstats $
```

---

### 4) Daytime protocol/Time protocol

Can use either the **Time protocol (Binary time stamps)** or **Daytime protocol (ASCII time stamp)** over Ethernet (similar to NTP). No password is required for these time stamps, unlike what is required for the CLI interfaces. Refer to “**Daytime and Time protocols (for all products)**” section in the CustAssist doc for more info: <..\CustomerServiceAssistance.pdf>

**Note:** These two Services are disabled by factory default. Must be enabled to use them

**Time protocol** = port 37

**Daytime protocol** = port 13

- Refer to **RFC 867** for more info on **Daytime** protocol: <https://tools.ietf.org/html/rfc867>
- Refer to **RFC 868** for more info on the **Time** protocol: <https://tools.ietf.org/html/rfc868>

#### When DayTime and/or Time protocols are enabled

- The associated service for Time/Daytime is **xinetd**, although this will launch Time/Daytime upon connection  
**xinetd** (per <https://en.wikipedia.org/wiki/Xinetd>)  
xinetd listens for incoming requests over a network and launches the appropriate [service](#) for that request.<sup>[5]</sup> Requests are made using [port numbers](#) as identifiers and xinetd usually launches another [daemon](#) to handle the request. It can be used to start services with both privileged and non-privileged port numbers.

- 
- 5) With Archive software versions 4.8.2 or higher, can also use **SNMP** to obtain the time (**ssSysStaDateTime**). Refer to the SNMP Application Note: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP](#)

---

## **\*\*IBM Model 9037 Sysplex timer (sysplex1) time stamps**

- Not available from base SecureSync
- Refer to the SecureSync Option Card document for info on Model 1204-02 RS-232 Input/Output Option Card.

---

## **\*\*\*PTP Output, IRIG output, ASCII output, etc**

- Refer to the SecureSync Option card info document

## **IPv6 support with PTP**

**(2 Aug 17, KW)** As of at least SecureSync version 5.7.0 (and timekeeper version 7.2.9), the SecureSync is not able to support IPv6 for PTP functionality (via the Option Cards or via the Timekeeper option). The 1204-12 and 1204-32 cards don't support IPv6, and timekeeper for SecureSync program does not currently support IPv6 with PTP, either

**Per Dave Sohn (1 Aug 17)** unfortunately, there is no current IPv6 support for PTP on SecureSync.

**Per Dave Sohn (2 Aug 17)** I'm confused as to how this would be a defect ticket, but certainly we'll add it as a feature request. VelaSync does not support IPv6 for PTP either.

---

## **\*\*1PPS output (on-time point /System 1PPS) / 1PPS generation**

### **1PPS output specs (for the base 1PPS output and 1PPS output Option Cards)**

- Excerpt below from the **online SecureSync user guide:**  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/OPTCARDS/OC\\_List/PPS\\_IO\\_10MHz.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPTCARDS/OC_List/PPS_IO_10MHz.htm)

### **1PPS Output Specifications**

- Signal Type and Connector: TTL level (BNC)
- Output Load Impedance: 50  $\Omega$
- **Rise Time to 90% of Level: <10 ns**
- Programmable Pulse Width: 100 ns to 900 ms with 20 ns resolution
- Absolute Phase Error:  $\pm 50$  ns ( $1\sigma$ )
- Programmable Phase Shift:  $\pm 5$ ns to 500 ms with 5ns resolution

### **1PPS TTL output voltage level/specs**

*From the SecureSync data sheet:*

|                                                                    |
|--------------------------------------------------------------------|
| <b>Signal Waveforms and Levels:</b> TTL (5v p-p), into 50 ohm, BNC |
|--------------------------------------------------------------------|

---

### **1PPS output Pulse Width**

**Q (from Salesforce Case 275427)** For the pulse width, do you know the tolerance of the setting. So for example, if the pulse width is set to 20 microseconds, do you know how close that value is actually coming in at? Is it +/- some value?

---

### **1PPS output Rise-time and Fall-time (base 1PPS output and all 1PPS output Option Cards)**

- (from the online SecureSync user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/OPTCARDS/OC\\_List/PPS\\_IO\\_10MHz.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPTCARDS/OC_List/PPS_IO_10MHz.htm))
  - **Rise Time to 90% of Level: <10 ns**
- 1PPS rise-times can be adversely affected by capacitance (not likely affected by cable termination)
  - Types of coax cable used can affect rise-time (low capacitance cable better for longer cable runs).
  - Extended lengths of cable can decrease rise-time
  - Inline splitters and inline amplifiers can affect rise-time

### **Customer reporting periodic 1PPS rise-times being slower than the normal ~200ns (such as 400ns)**

- Refer to Salesforce Case 217892

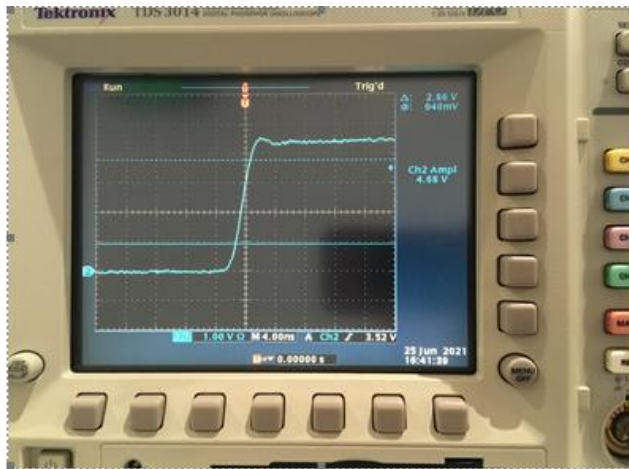
### Rise and Fall times between 20% and 80%? (versus 10% and 90%)

Q (from Salesforce Case 275427) Do you have a range for the Rise and Fall times between 20% and 80%? Your spec sheet says rise time is < 10 ns, but do you know what it is between 20% and 80%?

**Answer (per Tom Ellison, 23 Nov 2021)**

4.7 vdc amplitude(100%)  
3.8 vdc @(80%) dashed blue line  
0.94 vdc @(20%) solid blue line  
4ns scale per/div

**Answer ~ 2ns 20/80% rise time**



---

Q While looking through the user manual, I had some questions about the characteristics of the 1PPS signal that is provided on the SecureSync 1200. The manual talks about 4.3V, base to peak, but this does not tell me what is the minimum and maximum voltage?

Is the 1PPS signal synced to GPS time? So is the signal always sent out when GPS time ticks to a new second, or does it get sent out every second starting at some arbitrary time (i.e. at whatever time the system is started up)?

A Reply from Dave Lorah (21 Sept 15) The 1PPS signal is a TTL level signal. The base to peak difference is approximately 4.8 Vp-p into 50 ohms, the spec is 4.3 Vp-p minimum. The base being approximately 0 V.

The SecureSync will synchronize the 1PPS output to the GPS 1PPS Reference signal after the signal locks. When locked to the GPS signal the 1PPS output will be +/- 50 nS of the GPS 1PPS.

When the SecureSync first powers up the 1PPS will be arbitrary until it locks to the GPS (or any other ) reference source

---

### Desire for a 3.3v 1PPS output level

- Neither the base 1PPS and or any of the available 1PPS output Option Cards can provide a 3.3v 1PPS output signal.
- Recommend getting a fixed attenuator from Mini-Circuits (<http://www.minicircuits.com/homepage/homepage.html>) to be used external to the SecureSync.

Q According to SecureSync Instruction Manual, the minimum output Signal level is 4.3V minimum. I got 5.2V output when tested with the Oscilloscope, and I am wondering if this voltage is programmable to output around 3.3V?

**A (from Keith 29 Feb 16)** The SecureSync's 1PPS output is not adjustable in amplitude. There isn't an availability to provide a low voltage (3.3v) 1PPS signal directly from the SecureSync (via either the standard 1PPS connector on the chassis or via an installed Option Card providing a 1PPS output).

If a lower voltage signal is required, I recommend contacting Mini-circuits (<http://www.minicircuits.com/homepage/homepage.html>) to obtain a fixed attenuator to be applied external to the SecureSync itself to reduce the amplitude of the output signal as necessary for your particular application.

---

## 1PPS output configuration

Refer to online SecureSync user guide at:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/1PPS\\_outp\\_conf.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/1PPS_outp_conf.htm)

- Every base unit (including the Model 9489) has **one 1PPS** output ("PPS 0") on a BNC connector (this is a standard feature on all units).
- Can configure the 1PPS output for: Signature Control, Offset, active edge (Rising or Falling) and Pulse Width

### To configure the 1PPS output

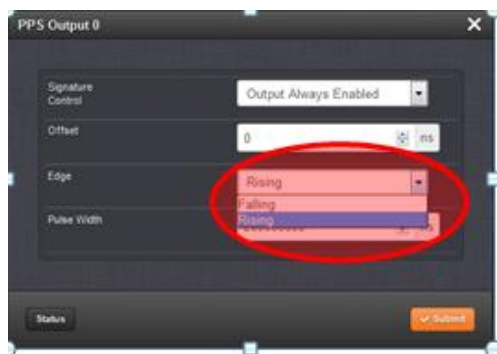
1. Navigate to the **Interfaces** -> **PPS Output** page of the browser (PPS output 0 for the base output)
2. Press **Edit**

### Desire to trigger on trailing/falling edge of the 1PPS output instead of rising edge

- The 1PPS signal can be inverted so that the ontime point (first/active edge) is Falling instead of Rising
- The data sheet's 1PPS output accuracy specs are the same whether the active edge is rising or falling.

### To configure the active (ontime) edge to be either the "Rising" edge (factory default) or "Falling" edge

- 1) Navigate to the **Interfaces** -> **PPS Output** page of the browser (PPS output 0 for the base output)
- 2) Press **Edit**
- 3) In the "**Edge**" field, select the desired edge (such as "Falling")



- 4) Press **Submit**

## 1PPS output Signature Control

**Your questions** (per Salesforce Case 232029, May 2020)

If we have vacant PPS ports, can we expect the ports are set to be working?

Is there any command or GUI check that we can see if a vacant PPC port is set to be working?

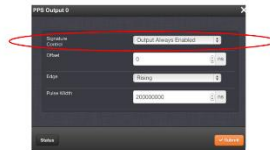
**Answer (reply from Keith, 11 May 2020)**

Yes! Every vacant 1PPS port (input and/or output) is available for your use.

By factory default (and unless a user has since re-configured the individual “**Signature Control**” setting for each 1PPS output port via the web browser) every 1PPS output (one port on the base chassis and all ports on installed 1PPS distribution Option Cards) is enabled and provides a 1PPS output signal.

For additional info on configuring 1PPS outputs, please also refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/1PPS\\_outp\\_conf.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/1PPS_outp_conf.htm)

The **Interfaces -> Outputs -> 1PPS output** pages of the SecureSync’s web browser allow each individual 1PPS output to be configured, as desired. The factory default value for this setting is “**Output Always Enabled**” As long as the “**Signature Control**” selection (as shown below) for each 1PPS output is still set to “**Output Always enabled**” (hasn’t since been changed by a user), the 1PPS output is enabled and the signal is available at the port.



**Note** “Signature Control” provides the optional ability to completely “squench” (stop) an output signal from being present on each output port, if the SecureSync doesn’t currently have an input reference present for the SecureSync to be in sync with. For more info on Signature Control settings please refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/Global/Topics/SETUP\\_Sha/Signature\\_Control.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/SETUP_Sha/Signature_Control.htm)

If the “Signature Control” value of any output has since been changed by a user to “**Output always disabled**”, the 1PPS signal will not currently be available on that 1PPS port, until the field has been reconfigured to a different selection. Or, if “Signature Control” value has since been changed to either of the other two available drop-down selections (“**Output enabled in Holdover**” or “**Output disabled in Holdover**”) the presence of the 1PPS signal on that particular output port is determined by the SecureSync’s current Sync status/whether the SecureSync currently at least one present/valid input reference for its synchronization.

In summary, all PPS ports configured as “**output always enabled**” will have a 1PPS output signal present at its port.

---

## 1PPS output termination

- Should be terminated into 50 ohms
- High impedance termination can cause ringing of the signal
- Refer to the oscilloscope photos for the difference between high z and 50 ohm termination: [!:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\1PPS Photos](#)

---

## 1PPS OFFSET: Internal/System delays of 1PPS (System Time)/

**Q** Is there any data about internal delays for 1PPS output? Manual says it’s a negligible, but is there any numerical value or estimate available?

**A** **Per Dave Sohn (22 May 2014)** We have tried to mitigate offset internal generations to minimize internal delays and propagation delays for the 1PPS. I don’t have a specific value for it. Our algorithm tracks the input reference, but is not directly tied to it.



## Whether to use positive or negative OFFSET value (from Case 259422)

**Email from Keith** Adding delay (Offset) compensation on the input reference that the SecureSync is synced with (such as GPS or IRIG input) will inherently move the SecureSync's System 1PPS and all its outputs by the Offset value entered (a positive value to push the 1PPS ahead, or negative to pull the 1PPS back). But if its desired to only offset one particular output (such as an IRIG output), the Offset should be configured for just that particular output.

A positive Offset value will "advance/forward" the 1PPS, while a "negative" Offset value will "retreat/retract" the 1PPS Offset. So, adding a positive 27000 ns Offset in the dedicated IRIG output going over to the other SecureSync will advance the 1PPS its providing by 27 microseconds. Adding a negative "27000" ns Offset will retreat the 1PPS of the IRIG by 27 microseconds.

If the 27 microseconds of offset is due to the coax cable delay between the IRIG out of the GPS-synced SecureSync to the other SecureSync, adding a positive 27000 ns of Offset to the IRIG output ([Interfaces -> IRIG out](#) page of the web browser) will "advance" the 1PPS of the IRIG output by 27 microseconds.

When the IRIG output signal reaches the secondary SecureSync, the advancing of the PPS (inside the GPS SecureSync) will have then been negated at the input of secondary SecureSync by the actual delay through the cable, resulting in the PPS of the IRIG output and the PPS of the IRIG input coincident with each other (as if they were directly connected to each other, instead of having a cable located between them).

---

## Effects of NTP peering on the oscillator/System PPS/1PPS outputs

- NTP peering is not recommended for use with Simulcast applications
- No matter which type oscillator is installed (TCXO, OCXO or RB), when NTP peering is used (such as loss of GPS reception for instance), the System 1PPS (and therefore 1PPS outputs also) is dithered to initially align it with the 1PPS obtained from NTP. I believe it's then periodically dithered to keep it aligned to the NTP 1PPS (in at least versions 5.2.1 and below, which don't discipline the oscillator when NTP is the selected reference. Host disciplining is in update version 5.3.0- Sept, 2015).
- The moving of the System PPS when peering is active adversely affects simulcast systems that are relying on a stable 1PPS output.
- The only input reference recommended for simulcast is GPS!

---

## Simple test using a multimeter to check for the presence of a 1PPS signal

- Refer to the "1PPS output" sections of the SecureSync Option Card assistance doc.
- Info in the Option Card doc is from Salesforce Case 280505.

## \*\*System Time Message Daemon\*\* function (STMD) (marker for the time to next 1PPS)

- New feature added in software version 5.2.0

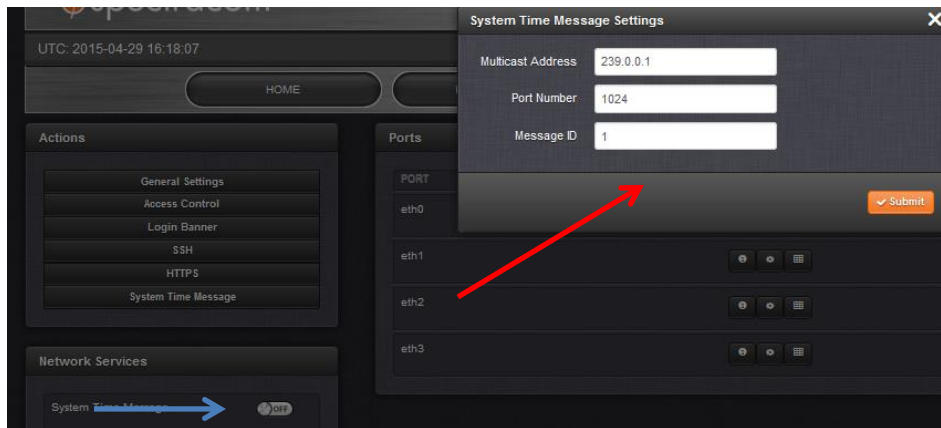
**Per Dave Sohn (29 Apr 15)** This existed in 5.2.0 as well. It was done for a specific customer, but could be used by anyone.

- Once-per-second message which reports which second the 1PPS is in (which second since Jan 1, 1970) and how far into the current second it is (such as 10ns for example) allowing how long to the next 1PPS easy to calculate.

I suspect this message may be used to help determine the accuracy of the 1PPS of an external device synced to the SecureSync. It helps verify if the external device is within the correct second (whether it's behind or ahead of the actual System PPS) and how closely aligned it is to the System PPS (in nanoseconds)

**Management** -> **Network** page of the browser

- Enable/Disable this service using the slider switch in the bottom left corner under “**Network services**”
- Configure this service by selecting the “**System Time Message**” button in the upper-left corner.



## System Time Message

- This message contains the time when the next 1 PPS discrete will occur. It is sent once per second prior to the 1 PPS discrete.

### System Time Message Format

| Word | Byte 3   | Byte 2 | Byte 1 | Byte 0 |
|------|----------|--------|--------|--------|
| 1    | Msg ID   |        |        |        |
| 2    | Msg Size |        |        |        |
| 3    | Seconds  |        |        |        |
| 4    | nSec     |        |        |        |
| 5    | EOM      |        |        |        |

### System Time Message Field Descriptions

| Data Name    | Data Description                                    | Range                   | Resolution | Units   |
|--------------|-----------------------------------------------------|-------------------------|------------|---------|
| Message ID   | UID of the message – desire this to be programmable | Unsigned 32 bit integer | 1          | n/a     |
| Message Size | Total message size in bytes                         | Unsigned 32 bit integer | 1          | Bytes   |
| Seconds      | Seconds since epoch (00:00:00 Jan 1, 1970 UTC)      | Unsigned 32 bit integer | 1          | Seconds |
| NSec         | NSec within the current second                      | Unsigned 32 bit integer | 1          | nsec    |
| EOM          | End-of-message                                      | -1                      | 1          | N/A     |

**Message ID:** An arbitrary number a user can select to send with the data message.

**Message Size:** I suspect this is the checksum so it can be determined if the entire message was received.

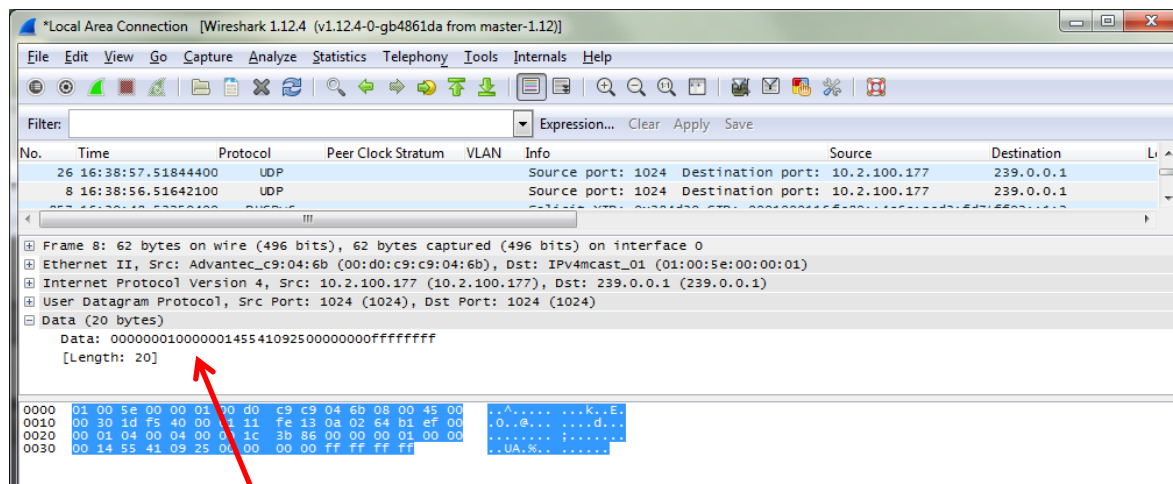
**Seconds' field:** I suspect this field may be used to help determine the accuracy of the 1PPS of an external device synced to the SecureSync.

**Nsec field:** is how far into the current second that the 1PPS is aligned to (in nanoseconds), which allows the ability to tell how closely aligned an external system syncing to the SecureSync is to the System PPS. It also allows easy calculation for when to expect the next system PPS to occur (if the field reports 10ns into the second, this indicates there is 990 ns till the next 1PPS on-time point).

**EOM field-** indicates the end of the message has been received.

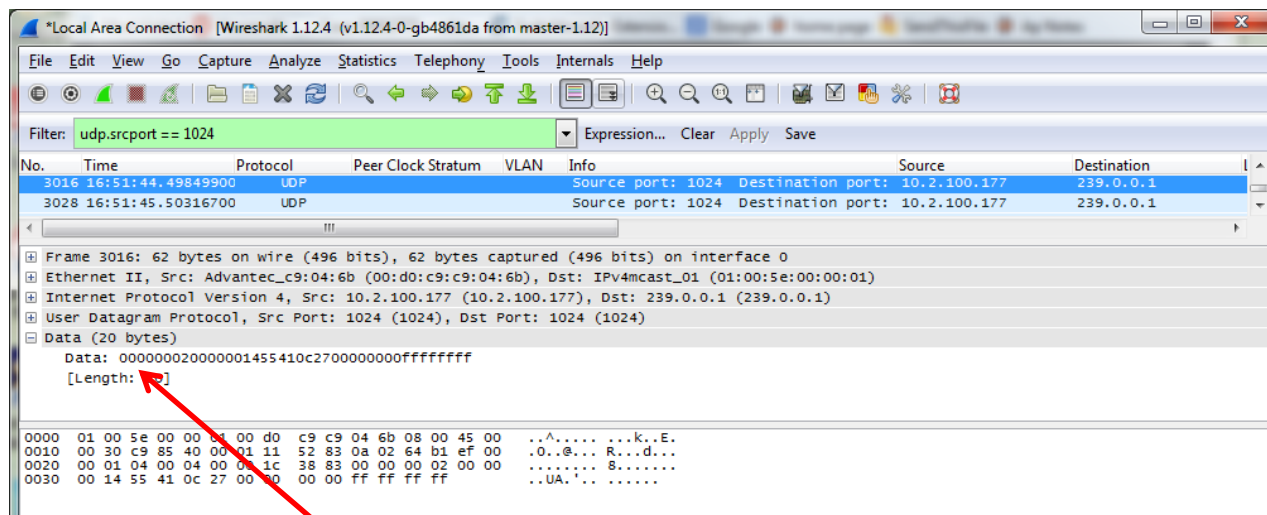
**Example messages:**

**Message ID 1**



Configured "Message ID" number ("1")

**Message ID 2**



Configured "Message ID" number ("2")



## Base 1PPS output Enable / Disable control using CLI “ppsctrl” command

- Version 4.8.7 (~Sept 2012) added ppsctrl command to enable or disable the 1PPS output on the rear panel

Q from BAE systems- Our requirement is to be able to Enable\Disable the 1PPS outputs programmatically. To do so, I use the CLI command ppsctrl. The question is, can the resultant output level of a disabled 1PPS control be programmatically set? Most times, when disabled it is 0V which is what we need. Sometimes though, it is 10V which is bad for us. It seems the level depends on where in the 1PPS pulse the output transitions to disabled.

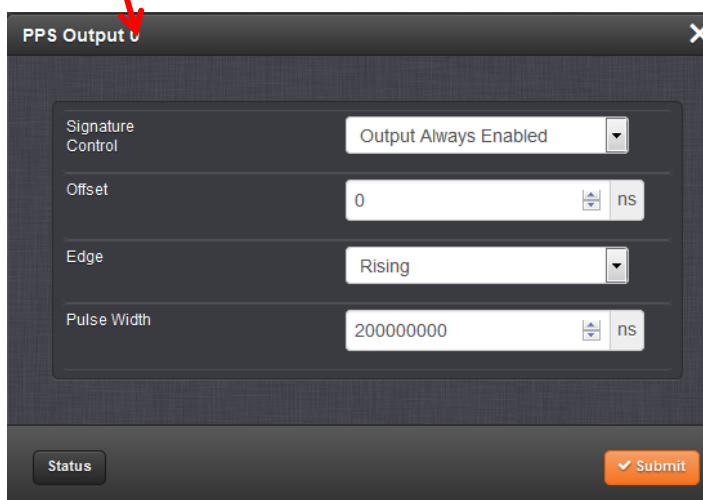
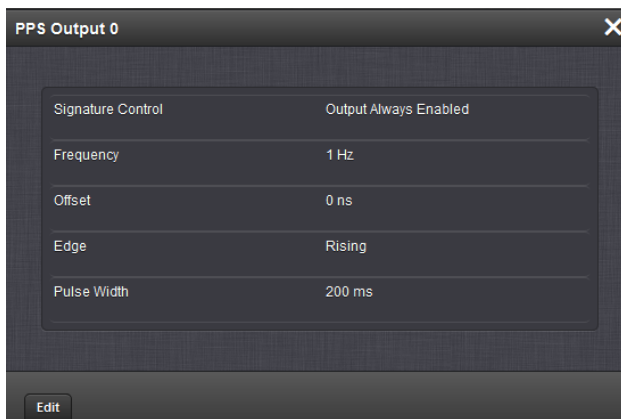
**A Per Dave Sohn 19 Mar 15:** “We currently freeze the output at the current level, I believe, and is played out according to your report. There isn’t a way to do what you want programmatically. However, depending on the responsiveness for your disable, you could perform the disable half way through the second, which would ensure that the 1PPS is already in its inactive state.

## 1PPS output configuration

- 1PPS out configuration consist of: Signature Control, Offset, Edge and Pulse Width

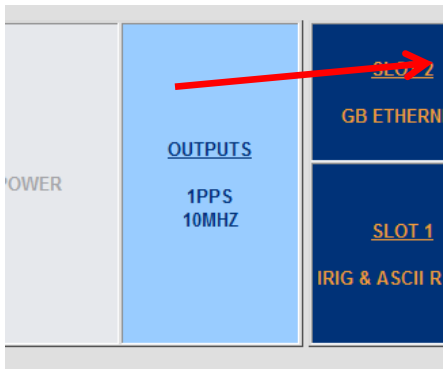
### A) Newer web browser

Interfaces -> Outputs -> PPS Output 0 page of the browser (see “Signature Control” below)



### B) Classic Interface (v5.0.2 and below)

Setup -> Outputs -> 1PPS 10MHz page of the browser, 1PPS tab



### ON-BOARD OUTPUTS SETUP

1PPS
10MHZ

|                   |                         |
|-------------------|-------------------------|
| Signature Control | Output Always Enabled ▾ |
| Edge              | Rising ▾                |
| Pulse Width (ns)  | 200000000               |
| Offset (ns)       | 0                       |

Submit
Reset

---

### 1PPS output Signature Control

Signature Control cannot take effect during power-up, until the software is operational. During initial power-up, the 1PPS output will be present. Once the software is running, the 1PPS output will then be suppressed, if Signature Control is enabled. There is no hardware Signature Control available to suppress the output upon initial power-up.

---

### 1PPS Pulse Width

- Default Pulse Width is 200 milliseconds wide.
- 1PPS output Pulse Width range (based on the web browser and info in the Option Card section of the manual): 20ns to 900ms.
- Configurable in the *Setup* -> *Outputs* -> *1PPS Frequency* page of the browser.

Q. Can SecureSync send 3.3v TTL by change of configuration parameter (Base PPS or Option Card)

A. **Reply from Dave Lorah (19 Apr 13)** The 1PPS TTL is based on a 5V signal level. This is true for the main chassis 1PPS signal and any option card 1PPS TTL outputs. There is one exception of the 1204-19 1PPS card, which is 10V level.

None of these has a 3.3V TTL signal. The 1PPS TTL levels are not adjustable and will always be 5V.

---

### 1PPS generation/1PPS alignment to 10 MHz

- Refer to the 10MHz output section for info regarding 10MHz and 1PPS phase alignment: [10 MHz phase alignment to 1PPS input reference](#)

---

### 1PPS output accuracy

- Typical specs (1-Sigma, which means on average, within 67% of the time during operation), from the SecureSync data sheet (values are oscillator dependent, when locked to GPS, and after for OCXO/Rbs, AFTER minimum oscillator wamup )

**1 PPS Output:**

|                                                | TCXO   | OCXO   | Low Phase Noise OCXO | Rubidium | Low Phase Noise Rubidium |
|------------------------------------------------|--------|--------|----------------------|----------|--------------------------|
| <b>Accuracy to UTC (1-sigma locked to GPS)</b> | ±50 ns | ±50 ns | ±25 ns               | ±25 ns   | ±25 ns                   |

**1PPS output offsets between more than one Securesyncs (synced via GNSS receiver)**

Q how tight can we get the 1PPS edge synchronized between remote locations, say 1km apart and connected by fiber optic?

**A Email from Keith to Wade Sober for his customer’s question (19 June 2019)** The specific answer to this question will likely be best answered by Dave S or Ron. But here goes my stab at it:

To begin, we don’t provide “absolute” worst-case 1PPS output specs, just typical estimations during normal operation, based on oscillator-type installed, and based on operation- such as locked to GPS for a specified minimum amount of warm-up time after each power-up..

|                                         | TCXO   | OCXO   | Phase Noise OCXO | Rubidium | Phase Noise Rubidium |
|-----------------------------------------|--------|--------|------------------|----------|----------------------|
| Accuracy to UTC (1-sigma locked to GPS) | ±50 ns | ±50 ns | ±25 ns           | ±25 ns   | ±25 ns               |

Going by the “typical” (1-Sigma, which means on average, within 67% of the time during operation) 1PPS specs in the SecureSync datasheet, the typical offset for each unit is +/- 50ns from UTC typical for OCXO or +/-25ns from UTC typical with Rb osc

This equates to the TYPICAL (average of 67% of the time) worst-case offset between the 1PPS outputs of two GNSS-synced SecureSync (no matter where they are located- whether miles apart or right next to each other) is either:

**typically, less than 100ns for OCXO or**

**typically, less than 50ns for Rb**

Note that 1PPS delays in the GPS antenna cable should be calculated/accounted for in all associated units, via the SecureSync’s browser, to help compensate for potential differences in these delays for each of the units. This will help to better optimize the alignments of 1PPS outputs from more than one SecureSync.

**1PPS output Holdover (System Time drift with no input references available)**

- Refer to: Oscillator Holdover specs (excerpt from the SecureSync datasheet)

## 1 PPS Output:

|                                                                       | TCXO   | OCXO   | Low Phase Noise OCXO | Rubidium | Low Phase Noise Rubidium |
|-----------------------------------------------------------------------|--------|--------|----------------------|----------|--------------------------|
| Accuracy to UTC (1-sigma locked to GPS)                               | ±50 ns | ±50 ns | ±25 ns               | ±25 ns   | ±25 ns                   |
| Holdover (constant temp after 2 weeks of GPS lock)                    |        |        |                      |          |                          |
| After 4 hours                                                         | 12 µs  | 1 µs   | 0.5 µs               | 0.2 µs   | 0.2 µs                   |
| After 24 hours                                                        | 450 µs | 25 µs  | 10 µs                | 1 µs     | 1 µs                     |
| Signal waveforms and levels: TTL (5V <sub>pp</sub> ) into 50 ohm, BNC |        |        |                      |          |                          |

### Other 1PPS output specs, besides accuracy

- 1PPS output connector specs from manual:

#### 1.7.5 1PPS Output

|                           |                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------|
| <b>Signal:</b>            | One pulse-per-second square wave derived from the GPS receiver.                           |
| <b>Signal Level:</b>      | TTL compatible, 4.3 V minimum, base-to-peak into 50 ohms.                                 |
| <b>Pulse Width:</b>       | Configurable Pulse Width (200 milliseconds by default).                                   |
| <b>Rise Time:</b>         | Approximately 2 nanoseconds                                                               |
| <b>Accuracy:</b>          | Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference. |
| <b>Connector:</b>         | BNC Female                                                                                |
| <b>Signature Control:</b> | Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference. |

#### Pulse rise time <4 ns

The 1PPS output from the main unit is ~2ns.

The 1PPS output from the 1204-01 option card is ~16ns.

#### Jitter <50 ps

The PLLs used in our FPGAs to generate the 1PPS outputs can have as much as ±2ns jitter (The following are the clocks used internally and the maximum PLL jitter: 10MHz = ±2ns, 50MHz = ±500ps, 200MHz = ±125ps)

#### Stability <20 ps / K between 20 ° C and 30 ° C ambient temperature

We don't have data on this, but the oscillators have the following specs over the entire operating range of the unit of the following (MP OCXO = 5ppb, HP OCXO = 1ppb, RbXO = 0.5ppb)

#### Pulse transit time difference between the outputs (output to output skew) <100ps

The 1PPS output from the main unit and 1204-01 option card are ~35ns apart, although that could be resolved to within 5ns.



Optional is a **configurable output frequency** of this reference pulse output by the user benefit. We are not sure what this means. The frequency of the 1PPS output is not configurable. However, the pulse width and active edge of the 1PPS can be configured.

---

## 1PPS output impedance

**Email from Mark McGregor about the SecureSync 1PPS output (11/22/10):** You are correct that the source/output impedance of the SecureSync 1PPS output is about 8 to 10 ohms. Our product data sheet does not state that the source impedance of the 1PPS output is 50 ohms. For 1PPS output it states "Signal Waveforms and levels: TTL (5Vp-p) into 50 ohm, BNC". See the bottom of page two on the attached product data sheet. This statement says that the SecureSync 1PPS output can drive a 50 ohm load. It does not say that the SecureSync 1PPS output is a 50 ohm source/output impedance. It should be corrected to say 4.3Vp-p, rather than 5Vp-p. The instruction manual has the 1PPS output voltage levels correct in section 1.7.5. I attach it here as well for your reference.

You can use the SecureSync source impedance of the 1PPS output in the voltage divider you outlined several emails down, but it is around 8 to 10 ohms. The 1PPS output is 4 each, 5V powered, ACT logic gates with a 4.75 ohm resistor in series with each gate output, connected in parallel at the 4.75 ohm resistor outputs to be able to source the current needed to drive 50 ohms. The 4.75 ohm resistors are all tied together to form the 1PPS output. You will have to adjust the "Rseries" up to account for the lower "Resource" to get the voltage divider you show several emails down to work the way you want it to.

Also, the 1PPS output is a fast rise time signal, ~2 nanoseconds into 50 ohm load, so in order to avoid large amounts of reflections/ringing the 1PPS output must be terminated with 50 ohms at the destination. If the 1PPS output is connected to a digital input that is a high impedance load there will be severe reflections/ringing. The scheme you showed should do that, more or less.

---

## 1PPS cable lengths

Q. How long can the RG-58 cable for the SecureSync's 1PPS output be to an SASe.

A. Reply from Dave Lorah on 9/16/11, based on engineering feedback:

We verified overnight running a 1PPS through a SAS synchronizing a SecureSync through around 800 feet of RG58 cabling. The maximum cable length is not determined. Hopefully 800 feet is longer than you need. Of course running through that much cable, you will have to compensate for the propagation delay of the cable and the effects of the slower rise time. The propagation delay of RG-58/U cable is about 1.51 ns/ft.

---

## Signature Control for various outputs (such as IRIG, 1PPS, 10 MHz, etc)

- Refer to (in SecureSync online manual):  
[http://manuals.spectracom.com/SS/Content/Global/Topics/SETUP\\_Sha/Signature\\_Control.htm?Highlight=signature%20control](http://manuals.spectracom.com/SS/Content/Global/Topics/SETUP_Sha/Signature_Control.htm?Highlight=signature%20control)

### Function of Signature Control

Signature Control is a user-set parameter that controls under which output states an output will be present. This feature allows you to determine how closely you want to link an output to the status of the active input reference e.g., by deactivating it after holdover expiration. It is also offers the capability to indirectly send an input-reference-lost-alarm to a downstream recipient via the presence of the signal.

The available options are:

- I. Output Always Enabled**—The output is present, even if SecureSync is not synchronized to its references (SecureSync is free running).
- II. Output Enabled in Holdover**—The output is present unless SecureSync is not synchronized to its references (SecureSync is in Holdover mode).
- III. Output Disabled in Holdover**—The 1PPS output is present unless the SecureSync references are considered not qualified and invalid (the output is NOT present while SecureSync is in Holdover mode.)
- IV. Output Always Disabled**—The output is never present, even if SecureSync references are present and valid.

*Signature control output-presence states*

| Ref. | Out-of-sync, no holdover | In holdover | In-sync with external reference |
|------|--------------------------|-------------|---------------------------------|
| I.   | ✓                        | ✓           | ✓                               |
| II.  | ✗                        | ✓           | ✓                               |
| III. | ✗                        | ✗           | ✓                               |
| IV.  | ✗                        | ✗           | ✗                               |

## **\*\*10 MHz output(s)**

### **Number of 10 MHz outputs**

- (Except 9489) Base unit has one 10MHz out.

### **Available Option Card for 3 additional 10 MHz outputs**

- Refer also to: <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>
- **Models**
  - **1204-1C** (current version)
  - **1204-0C** (no longer available – replaced by the 1204-1C)

---

## **10 MHz Output signal levels/amplitude (base unit and 1204-1C option card)**

**Output signal:** Sinewave

- **From SecureSync data sheet:** +13 dBm (+/- 2dB) into 50 ohm, BNC (11 dBm= 2.85vpp 15 dBm=4.5vpp)
- Output level/gain is not adjustable inside the SecureSync.
- Use external line attenuators, if amplitude into 50 ohm input impedance is too high.

**Output impedance:** 50 ohms

### **Resistor change to increase output amplitude**

- Refer to ECO-002802 (in Arena): [https://app.bom.com/changes/detail-summary?change\\_id=2408423708&](https://app.bom.com/changes/detail-summary?change_id=2408423708&)

**Description:** Update all SecureSync 1200 Rubidium option top level BOM for R164 resistor change to correct 10 MHz output amplitude is too low.

This ECO changes R164 to new part R116R-48R7-YF0B for all SecureSync 1200 Rubidium option top level BOM.

This is a corrective action for CAPA-000134.

---

## **Simulcast radio system terminations**

- Also refer to the “Simulcast radio systems 10 MHz inputs” section of the the Custserviceassistance doc

Q. How many base stations can the 10mhz output port successfully drive?

**A. Reply from Ed O'Connor (8 Dec 16)** In general for some bases (such as Moto GTR8000, Harris Mastr 3, Kenwood NXR700/800) our output should drives just one base since 10MHz input on those bases have a 50 ohm termination. We can probably successfully drive 2 bases, it is up to the customer to verify, and I discourage any more than 2 bases

10MHz input on Tait bases has a high-z impedance. I have heard of customers driving 7-8 base stations off a single 10MHz output

---

## **10 MHZ frequency Offset**

(As of at least Nov 2012, Archive version 4.8.7 and below) Unlike the Model 8195 series Master Oscillators had the ability to offset the 10 MHz output by a specific value (using the 1FO command).This capability was not carried over to the SecureSync and 9400 series.

Ed O'Connor said today he may consider seeing it added with the "cleanup" oscillator, but it's not currently available.

---

## \*\*\*\*10 MHz phase alignment to 1PPS input reference/discontinuities between 10MHz vs 1PPS/1MHz and 5 MHz outputs

### 1PPS generation

- Except after boot-up, there are always 10,000,000 frequency counts between each 1PPS.

**Note:** (2 Jan 2014) Curtis Somers reported they observed an extra count, especially when going into Holdover mode. (Refer to Salesforce case 12863)

Reference Salesforce Case 231847 (May 2020)

### My response

The SecureSync's 10MHz oscillator is the core timing that is disciplined to the selected external input reference (such as the SecureSync's GNSS receiver's 1PPS output, for instance). The System 1PPS, 1MHz outputs, and 5MHz outputs are all derived from this disciplined 10 MHz signal.

The only time there are any discontinuities between the 10MHz and these other system signals/outputs is:

**At initial system Sync** (the first time after each system boot-up that an external input reference, such as the GNSS receiver, becomes present and valid for synchronization).

- 1) **Restarts of oscillator disciplining** (via either "**Restart Tracking**" which requires manual intervention, or via "**Phase error limit**" which is automatic, if configured).
- 2) **If/when Smart Reference Monitoring (also referred to as "Smart Phase Validation") is enabled and kicks in**, which disqualifies the input reference, resulting in another present/valid lower priority input reference to be selected. Or, if there are no other input references available, places the 10MHz oscillator in a free run (undisciplined state) state.

For more information on the available manual intervention **Restart Tracking** and automatic "**Phase Error Limit**", please refer to the online SecureSync user guide at:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/OscConfiguring.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm)

For more information on the available "**Smart Reference Monitoring**" ("Smart Phase Validation"), including how to enable it via the SecureSync's web browser, please refer to the online SecureSync user guide at:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/TIME/RefMon.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/RefMon.htm)

In summary, SecureSync doesn't make phase steps compared to the 10MHz signal after oscillator lock, unless phase validation kicks in. Instead, the SecureSync disciplines its 10MHz oscillator's output frequency, which drives the 1PPS, 1 MHz and 5MHz outputs, as they are all derived from it.

---

### Questions from a customer (refer to SF case 95886)

1. Is it possible to get the 1PPS rising edge 10-20 ns before the 10MHz rising edge with the SecureSync?
2. Is there a relationship between Phase Error and the 1PPS/10MHz skew?

The relationship between the rising edge of 1PPS and the rising edge of 10MHz is unclear to me based on the SecureSync User Reference Guide Rev 23.

Scope measurement shows the 1PPS and 10MHz rising edges are not aligned. Also the Phase Error relationship to this 1PPS/10MHz skew is unclear.

We coded some VHDL assuming the 1PPS comes after the 10MHz (not before) so we may need to change some VHDL for the FPGA based on your response.

**A REPLY FROM Jodi, after working with Tom Richardson (18 Jul 17)** I consulted with an Engineer yesterday about your questions. A SecureSync unit in the lab was tested, and the 1PPS rising edge was coincident with the 10 MHz rising edge with 1PPS offset set to 0. You should be able to use the offset setting in the 1PPS setup page to delay the 1PPS by 20 nSec. We have set the offset to 20 nSec on this device and the 1PPS moved 20 nSec earlier than the 10 MHz rising edge.

Also, are you using matched length cables? Cable delay is about a nanosecond per foot of coaxial cable. Another way to get a 20 nSec delay in the 1PPS is to add about 20 feet of coaxial cable to the output of the 1PPS. The resolution of the adjustment of the 1PPS offset should be approximately 5 nanoseconds so you could fine adjust by changing the length of a coaxial cable acting as a delay line.

There should always be 10 million cycles of the 10 MHz between the 1PPS output. The phase error relationship between the 1PPS and the 10 MHz should always be a fixed amount. In other words they move together when the 10 MHz is adjusted.

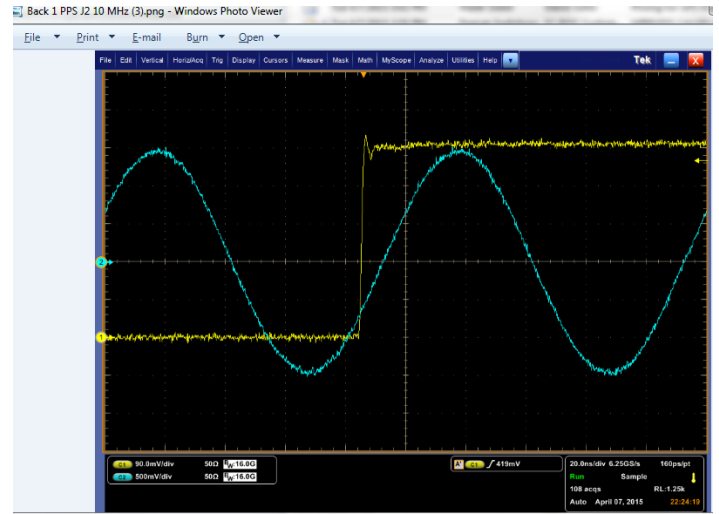
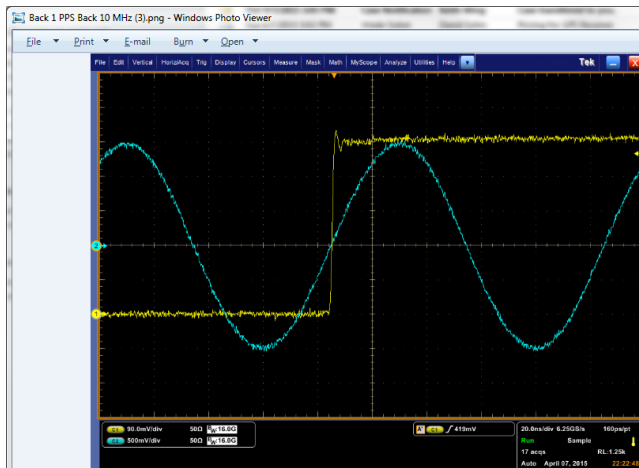
---

### **1PPS / 10 MHz alignment at the base 10 MHz output port versus all the 1204-1C Option Card outputs**

- Refer to Salesforce case 17618.
- 1PPS /10 MHz alignment at the base 10 MHz output port is slightly different on the 1204-1C 10MHz output Option Cards
- 1PPS /10 MHz alignment at the base 10 MHz output port is the same as the outputs of the earlier 1204-0C 10 MHz Option Cards.
- This is due to the 10 MHz distribution for the base output port being different than the 1204-1C Cards.

**1PPS/10MHz alignment for base output (and 1204-0C 10 MHz Option Cards)**

**1PPS/10MHz alignment for all 1204-1C option Card outputs**



**Per Dave Sohn (7 Apr 2015)** This is what I would expect from the system. There is no HW issue. The phase relationship on a 10MHz output is fixed with the 1PPS, but there is a difference between the outputs on the option card versus the main unit. If they need multiple outputs that have the same phase relationship, then they can just use the 1C option card outputs.

**Dave Sohn responded with:** This specification is held once HW adjustments are disabled after first sync (or if restart tracking is sent). At this point, the 1PPS is generated directly from the 200Hz clock, which is generated through a PLL from the 10MHz. However, when going into holdover, the 10MHz frequency will change from the current correction frequency to our best estimate of the correct frequency without any corrections for phase errors. It's possible that with that change, the 1PPS may appear to have one extra cycle if an edge transitioned later because of the frequency change and how their counter is tracking it and the 1PPS.

### Phase alignment of 10 MHz outputs from multiple TSync-PCIe boards or SecureSyncs

Because KTS disciplining performs phase alignment of the 10 MHz output, unlike earlier NetClocks which only perform Frequency adjustments, if more than one TSync or SecureSync are synced to the same IRIG or GPS signal, the 10 MHz outputs will be in phase with each other (not just corrected for frequency).

**Frequency Accuracy Error** can be viewed to see if the 10 MHz oscillator is adjusting to the input reference (should continue to decrease on as it gets closer). The current **Frequency Accuracy Error** can be viewed in the **Status ->Time and Frequency** page.

#### **Email from Dave Sohn (12/13/11):**

"Synchronization works in SecureSync by trying to adjust the oscillator frequency to match the system's 1PPS in phase and frequency to the reference source. By matching the system 1PPS phase, which is aligned to the 10MHz on-board, we also get some phase alignment of the 10MHz signal itself. In order to match phase and frequency, each unit will be making adjustments to the frequency of the internal 10MHz oscillator. There is a maximum adjustment that can be made each second, and a maximum adjustment that can be made overall to limit the frequency error generated by the disciplining itself. There is also a limit as to the minimum adjustment our disciplining system to help reduce adjustments for very accurate references to minimize issues.possible to the oscillator frequency. That is a factor of the oscillator's control voltage range, pullability, and the precision of our DAC. Typically, for a HP (High Performance) OCXO the minimum adjustment we can do is 0.000015 Hz, which when multiplied up to their 3GHz frequency is 0.0046 Hz.

We are already working on improvements to our disciplining system to help reduce adjustments for very accurate references to minimize issues.

### Desire to phase align the 10 MHz of more than one SecureSync when using IRIG input for synchronization of the SecureSyncs.

- We recommend using IRIG DCLS input (not IRIG AM) for optimum phase alignment (DCLS has a faster rise-time

than AM, so it has a “crisper” on-time point).

- We don't recommend using IRIG A input, for optimum phase alignment.
- As long as all SecureSyncs are synced to the same IRIG source, their 10 MHz outputs should be fairly closely phase-aligned with each other

**Email from Sam Otto to Leisa Butler after taking to Denis Reilly (26 Mar 2013)**

Once the 1PPS signal from the IRIG DCLS signal is locked by the oscillator (OCXO or Rb) the 10MHz will be in Sync and in phase with it.

**We do not recommend IRIG-A.**

The same IRIG DCLS Signal will suffice as long as both SecureSyncs oscillators are in sync with the same IRIG DCLS signal their respective 10MHZ outputs will be in phase.

This can be verified by going to both SecureSync Status pages and selecting “**Time and Frequency**” and verifying that the “**Oscillator State**” is “**Track/Lock**”.

| TIME AND FREQUENCY STATUS      |                       |
|--------------------------------|-----------------------|
| Selected Time Reference Source | GPS 0                 |
| Selected 1PPS Reference Source | GPS 0                 |
| Synchronization                | OK                    |
| Holdover                       | Not in Holdover       |
| Time Figure of Merit (TFOM)    | 3                     |
| Estimated Time Error (ETE)     | 10 ns < ETE <= 100 ns |
| TimeScale Reference            | UTC                   |
| Oscillator Type                | OCXO (1ppb)           |
| Oscillator State               | Track/Lock            |
| 1PPS Phase Error (ps)          | 15                    |
| 10MHz Frequency Error          | 3.16e-11              |

Q. How closely are the 10MHZ and the 1PPS slaved together?

A. Except during power-up, there are always 10 million cycles of 10MHz between each 1PPS.

**Additional response from Denis Reilly (8 Oct 201)** “Further info (probably more than the customer needs at the moment):”

Except during power-up, there are always 10 million cycles of 10MHz between each 1PPS. After a reboot or power cycle, when the SecureSync syncs to a reference for the first time, the 1PPS and 10MHz are not guaranteed to be locked together during tracking setup.

When the Disciplining State transitions to “Locked”, we lock the 1PPS and 10MHz together, and guarantee that there will be 10 million clock cycles between PPS's as long as the Disciplining State remains “Locked”. (We can keep both the 10 MHz and 1PPS synchronized to the reference in this state without slipping the signals relative to each other.)

If a unit loses all of its references, and the holdover timeout expires, and the unit enters the Freerun state for a long time, there is a chance that upon acquiring a reference again the relationship between the 10MHz and 1PPS may drift again. But once the disciplining state becomes “Locked” again, the 10 MHz and 1PPS will be locked together again, and there will be exactly 10 million 10MHz cycles in between PPS's.

**Email from Dave Lorah (18 Nov 2013)** The SecureSync 1PPS is derived from the 10 MHz, so it should not be wandering at all. I think your scope may be set at the wrong horizontal time base and aliasing the 10 MHz signal. I could reproduce this on my scope too if using a millisecond per division range.

Switch to a 20ns/div scale and the 10 MHz should be locked on.

Please let me know if you see anything different.

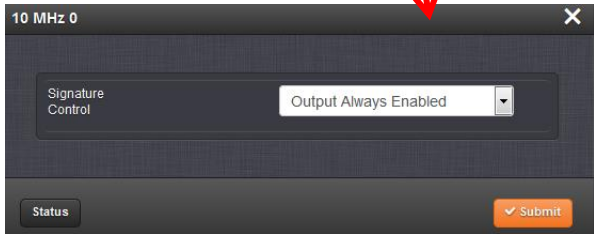
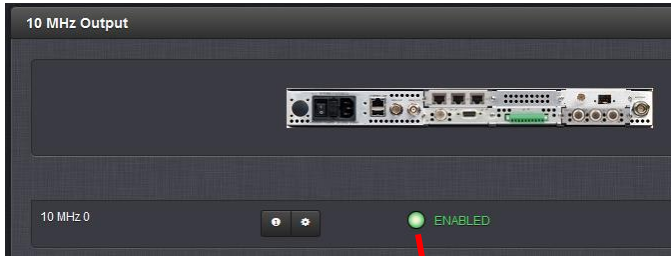
---

## 10 MHz output configuration

- 10 MHz out configuration is limited to just Signature Control

### A) Newer web browser

Interfaces -> Outputs -> 10 MHz Output page of the browser (see "Signature Control" below)



### B) Classic Interface

Setup -> Outputs -> 1PPS/ 10MHz page of the browser, 10 MHz tab





---

## \*\*\*\*10 MHz output Signature Control

**(11 March 2020) Note about SecureSync LPN Specials having a Wentzel oscillator installed, such as the SPECIAL Clock Generation Unit (CGU) for Hughes**

- Apparently, due to design changes needing to be incorporated to add the Wentzel LPN oscillator, 10MHz Signature Control is still displayed in the web browser. But it's not functional.

**Email from Dave L (11 March 2020)** This is confirmed to be a limitation of the product design. Incorporating the low phase noise oscillator feature has disabled the Signature Control function.

The SecureSync has a feature that can be enabled, which squelches the 10 MHz output when either the SecureSync's Sync state is not "true" OR when the SecureSync has no valid input references present (depending on how this mode is configured). This mode is called "**Signature Control**".

Signature Control can be enabled in SecureSync (it is disabled by default) using the web browser. Navigate to the **Setup-> Outputs -> "1PPS 10MHz"** page of the browser. Configure the "**Signature Control**" field as desired. The available selections are defined below:

- "**Output Always Enabled**": 10 MHz output is always present (no matter the Sync status or whether input references are present and valid)
- "**Output enabled in Holdover**": 10 MHz output is only present when the SecureSync is either in the Sync or Holdover modes.
- "**Output Disabled in Holdover**": 10 MHz output is only outputted when the TSync board has a valid input reference present.
- "**Output Always Enabled**": 10 MHz output is never present.

### Signature Control during SecureSync power-up

Signature Control cannot take effect during power-up, until the software is operational. During initial power-up, the 10MHz output will be present. Once the software is running, the 10MHz output will then be suppressed, if Signature Control is enabled. There is no hardware Signature Control available to suppress the output upon initial power-up.

---

## \*\*\*10 MHz output Phase noise / Harmonics/ spurs

**SecureSync/Models 9483 and 9489:** Refer to datasheet for phase noise and harmonics measurements/specs: [I:\Marketing\ Product Data Sheets \(archive\)\Time & Frequency References](I:\Marketing\ Product Data Sheets (archive)\Time & Frequency References)

**Note:** The low phase noise oscillator is not available with the Model 9400 series NetClocks.

**Phase noise measurements:** Refer to SecureSync data sheet. Per Mark McGregor, phase noise specs are for all 10 MHz outputs (the base 10 MHz as well as 10MHz outputs from installed 10MHz output Option Cards).

Mark also said this doesn't apply to 5MHz or other output Option Cards, because of the dividers used to generate the smaller frequencies cause a great amount of phase noise.

**Harmonics** (From the SecureSync manual)

|                   |                  |
|-------------------|------------------|
| <b>Harmonics:</b> | -40 dBc minimum. |
| <b>Spurious:</b>  | -70 dBc minimum. |

For plots of the 10 MHz harmonics and spurs with an OCXO installed, refer to the email from Tom Richardson (8/2/12) in the following folder: [EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSYNC-PCIe\10MHz output](#)

**Phase noise specs at 100 KHz (“@100 KHz”)**

- SecureSync data sheet doesn’t provide phase noise specs for @100 KHz (10 KHz is highest)
- Per Tom Richardson, the phase noise at 100 KHz is very similar to, or just slightly better, than the phase noise at 10 KHz.

Q. from Danny Loke Can you help me to find out the specs of phase noise of LN OCXO and Rb @ offset 100kHz?

A The phase noise specs for all of the various SecureSync oscillator configurations are in a table on page 2 of the SecureSync data sheet (attached).

On the left side, scroll down to “Phase Noise” as excerpted below:

|                             | TCXO | OCXO | Low Phase Noise OCXO | Rubidium | Low Phase Noise Rubidium |
|-----------------------------|------|------|----------------------|----------|--------------------------|
| <b>Phase Noise (dBc/Hz)</b> |      |      |                      |          |                          |
| @1 Hz                       | —    | -95  | -100                 | -80      | -100                     |
| @10 Hz                      | —    | -123 | -128                 | -98      | -128                     |
| @100 Hz                     | -110 | -140 | -148                 | -120     | -148                     |
| @1 KHz                      | -135 | -145 | -153                 | -140     | -153                     |
| @10 KHz                     | -140 | -150 | -155                 | -140     | -155                     |

Though we don’t spec the phase noise at 100 kHz, I spoke to one of our engineers that normally performs the phase noise testing. He said the phase noise at 100 kHz is very similar to, or just slightly better, than the phase noise at 10 KHz.

## Allan Deviation/Allan Variance (oscillator's output)

- Refer to the following link for the plots referenced below: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Allen Deviation plots
- Refer to the SecureSync data sheet for specs (also in online 1200 S/S manual at: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/SS/Topics/INTRO/Specs\\_10MHzOut.htm?Highlight=allan%20variance](http://manuals.spectracom.com/SS/Content/NC_and_SS/SS/Topics/INTRO/Specs_10MHzOut.htm?Highlight=allan%20variance))

10 MHz output — oscillator stability

| Oscillator Type             | Medium-Term Stability<br>(without GPS after 2 weeks of<br>GPS lock) | Short-Term Stability (Allan<br>variance) |                     |                     | Temperature<br>Stability<br>(p-p) |
|-----------------------------|---------------------------------------------------------------------|------------------------------------------|---------------------|---------------------|-----------------------------------|
|                             |                                                                     | 1 sec.                                   | 10 sec.             | 100 sec.            |                                   |
| Low-phase noise<br>Rubidium | $5 \times 10^{-11}$ /month ( $3 \times 10^{-11}$ /month<br>typical) | $5 \times 10^{-11}$                      | $2 \times 10^{-11}$ | $5 \times 10^{-12}$ | $1 \times 10^{-10}$               |
| Rubidium                    | $5 \times 10^{-11}$ /month ( $3 \times 10^{-11}$ /month<br>typical) | $2 \times 10^{-11}$                      | $2 \times 10^{-12}$ | $2 \times 10^{-12}$ | $1 \times 10^{-10}$               |
| Low-phase noise<br>OCXO     | $2 \times 10^{-10}$ /day                                            | $5 \times 10^{-11}$                      | $2 \times 10^{-11}$ | $1 \times 10^{-11}$ | $1 \times 10^{-9}$                |
| OCXO                        | $5 \times 10^{-10}$ /day                                            | $5 \times 10^{-10}$                      | $5 \times 10^{-11}$ | $1 \times 10^{-11}$ | $5 \times 10^{-9}$                |
| TCXO                        | $1 \times 10^{-8}$ /day                                             | $2 \times 10^{-9}$                       | $1 \times 10^{-9}$  | $3 \times 10^{-10}$ | $1 \times 10^{-6}$                |

Per Wikipedia: [https://en.wikipedia.org/wiki/Allan\\_variance](https://en.wikipedia.org/wiki/Allan_variance)

The **Allan variance (AVAR)**, also known as **two-sample variance**, is a measure of frequency stability in clocks. The *Allan variance* is intended to estimate stability due to noise processes and not that of systematic errors or imperfections such as frequency drift or temperature effects. The Allan variance and Allan deviation describe frequency stability. See also the section entitled "Interpretation of value" below.

### Email from Dave Lorah to Mark Goldage with GE (14 Feb 2013)

I had to consult engineering for this data. I think this is what you are looking for.

Here is an Allan deviation plot and a histogram of 5 days of a 9483 TCXO unit with GPS reference. This is 495634 seconds of data taken once per second.

The histogram shows a standard deviation of  $8.5 \times 10^{-8}$ , so 3 stds would be  $2.55 \times 10^{-7}$ , so uncertainty would be 10 MHz +/- 2.55Hz. The Allan deviation plot is a measure of the stability over observation time. This shows that for an observation time of  $6.55 \times 10^4$  (18 hours) the stability is about 2 parts in  $10^{-12}$ .

## Report of Allan Variance/Allan Deviation failing customer testing

- Refer to Salesforce case 171261 (9 Aug 2018)

**Email from Tom Richardson (9 aug 18)** Get the test methodology and equipment used if possible. Also what rev the software was at.

These specs are by design and we do not 100% test our product for these specifications. If they want it I think there is an additional charge.

**My reply to the customer (9 Aug 18)** about the specific report, before just assigning an RMA for the two SecureSyncs to be returned to Spectracom. We have some questions/requests for you, based on the specific failure report.

There are some "variables" which can affect Allan Variance test results. Environmental/temperatures during the testing is one (were the units allowed to warm-up/stabilize before any testing was started? Did the ambient temperature remain consistent through the test?, etc). Another "variable" is the version of software installed in the SecureSync, when the

testing was performed. What is the version of software installed in the two SecureSyncs?

If you aren't sure what version of software is currently installed, there are a few different ways to obtain the version: Note the software version of the **SecureSync** will be either a 4.x.x or 5.x.x number:

- Via the front panel keypad/LCD display (**System** -> **Vers** menus)
- With a CLI connection (telnet, ssh or front panel RS-232 cable) type: **version** <enter>. The version command will respond with the current version of software installed.
- With the newer black and charcoal web browser (starting in software version 5.1.2), the System version is reported in the **Tools** -> **Upgrade/Backup** page.
- With earlier software versions (which the web browser has a white/gray background and is now referred to as the "classic interface") the Archive software version is reported at the top of the **Tools** -> **Versions** page.

If addition to letting us know the installed version of software, can you also send us the test methodology/environmental conditions during the testing, what test equipment was used to perform the Allan deviation testing, test reports, etc. If possible, we would like to take a look at as much info you can provide us with about the actual testing, before just having the units returned to us.

Thanks very much in advance (if its not too much inconvenience) for providing us with as much of the above info you can. Then we can go from there 😊!

## 1PPS output phase noise

Email from John Westwood to Tom Richardson, (based on his testing)  
 Here is the measured 1ppS data, measured on an OCXO SS with GPS control.

| Tau S | ADEV    |
|-------|---------|
| 10    | 7E-11   |
| 20    | 4E-11   |
| 40    | 3E-11   |
| 70    | 3.5E-11 |
| 100   | 3.5E-11 |
| 200   | 3E-11   |
| 400   | 2E-11   |
| 700   | 1.5E-11 |
| 1K    | 9E-12   |
| 2K    | 5E-12   |
| 4K    | 2.5E-12 |
| 7K    | 1.5E-12 |
| 10K   | 0.9E-12 |
| 20K   | 0.9E-12 |

I will set this up for an extended run (this was 65 hours).

**Second email from John Westwood 11 Feb 2013** Here are the ADEV measurements over 7 days, this time with our Cesium as a reference – previous data was with the internal Rb reference (no GPS on this STA-61).

| Tau S | ADEV  |
|-------|-------|
| 1     | 4E-10 |
| 2     | 2E-10 |
| 5     | 9E-11 |
| 10    | 5E-11 |
| 20    | 3E-11 |
| 50    | 3E-11 |
| 100   | 4E-11 |
| 200   | 3E-11 |
| 500   | 2E-11 |
| 1K    | 8E-12 |
| 2K    | 5E-12 |
| 5K    | 2E-12 |
| 10K   | 9E-13 |
| 20K   | 5E-13 |
| 30K   | 4E-13 |
| 40K   | 3E-13 |

Very similar results up to 10K.

**Another email from John Westwood (18 Feb 2013):** Here are the results for both 4.8.7 and 4.8.8 software versions SecureSync 1200-013 with continuous GPS control Running for >7 days before start of collection 1ppS Adev measured on STA-61 with Cesium reference 1 second sample rate - run time 7 days

| S/W Version | 4.8.7     | 4.8.8     |
|-------------|-----------|-----------|
| Tau S       | 1ppS ADEV | 1ppS ADEV |
| 1           | 4.00E-10  | 4.00E-10  |
| 2           | 2.00E-10  | 2.00E-10  |
| 5           | 9.00E-11  | 8.00E-11  |
| 10          | 5.00E-11  | 3.50E-11  |
| 20          | 3.00E-11  | 2.50E-11  |
| 50          | 3.00E-11  | 1.00E-11  |
| 100         | 4.00E-11  | 8.00E-12  |
| 200         | 3.00E-11  | 8.00E-12  |
| 500         | 2.00E-11  | 1.00E-11  |
| 1000        | 8.00E-12  | 9.00E-12  |
| 2000        | 5.00E-12  | 7.00E-12  |
| 5000        | 2.00E-12  | 5.50E-12  |
| 10000       | 9.00E-13  | 4.00E-12  |
| 20000       | 5.00E-13  | 2.00E-12  |
| 30000       | 4.00E-13  | 1.20E-12  |
| 40000       | 3.00E-13  |           |

The 4.8.8 version has improved between 50 and 1000 seconds but is worse greater than 1000 seconds.

FYI: After changing to 4.8.8, the oscillator log does not show any DAC values, only frequency calculations.

---

#### \*\*\*\*Oscillator warm-up time

- **OCXO oscillators for TSync:** Warm-up time is about one (1) minute
- OCXO oscillators for SecureSync: Warm-up time is (3) minutes
- **Rb oscillator:** Warm-up time is about ten (10) minutes.

**Note:** The outputs will be stable after the warm-up time but will not be locked.

#### \*\*\*\*Frequency Accuracy error measurements

Calculated Frequency error (versus desired 10.00000MHz) is displayed on the **Status ->Time and Frequency** page of the web browser.

##### **Operation:**

Shortly after the **first** time the NTP server powers up, the 10MHz oscillator goes through an auto-calibration procedure. During this time-frame, the oscillator is directed to each of its steerable limits for about 5 seconds each with a couple of seconds of delay so the oscillator can stabilize (The whole oscillator calibration process takes about 20 seconds or so to complete). The Hertz range is stored in memory, so it doesn't need to auto-cal after subsequent reboots.

This allows the oscillator's Hertz Range and step sizes to be calculate and calibrated. Once the calibration process has been completed, the estimated D/A for a 10MHZ output is set and the oscillator is steered to this value. Thereafter, the frequency counts oscillator disciplining can begin (assuming the external reference- IRIG in this case- is present).

As for the amount of time it will take for the oscillator to settle out after power-up, the type of oscillator will have a significant factor in how long it takes to clear the alarm. The operation of the oscillator monitoring circuit for performing the frequency counts of the oscillator's output varies depending on the type of oscillator. With a TCXO oscillator, the frequency measurements and adjustments of the D/A occur every 1000 seconds (about every 18 minutes). After each frequency count, the D/A is adjusted and the frequency count is logged in the Oscillator log (Status and Logs/Oscillator log page of the web browser). In order for the Frequency alarm to clear, the Fractional Frequency Error (labeled in this log as "Freq Error") has to be better than  $1 \times 10^{-7}$ . Each frequency count should decrease the Freq Error value, bringing it closer to this value. By looking at these measurements in the Oscillator log, you can determine how close it currently is and be able to obtain a pretty good idea of about how long it will take to reach this minimum criteria threshold.

Typical time after each power-up for OCXO to be within our specs: about 10 minutes total

**Note:** Per our test data sheet, the acceptable range on the 10 MHz output amplitude is 2.2 to 3.6vpp.

#### **OCXO oscillator free-run (holdover)**

**Email from Dave Sohn (10/3/11):** The 10MHz drift is entirely based on the aging rate of  $2E-10$ /day.

---

#### \*\*\*\*10 MHz stability after power-up

- A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.

**Email from Dick Fox to a customer (6/10/12)** To obtain predictable drift rates for Rubidium Oscillators you need to:

- Keep the units powered. Temperature stability is a major factor in determining the accuracy so once powered you need to keep them powered
- A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.
  - A. Secure Sync sets a DAC value that controls the frequency of the Rubidium Oscillator
  - B. SecureSync must be synchronized to GPS for a minimum 24 hours before the DAC value is set.**
- Secure Sync will not make any changes to this DAC value unless SS is synchronized to GPS for 24 hours or

more.

- This mean that short GPS syncs will NOT reset the Rubidium frequency and its drift. But short GPS syncs will correct the time offsets.
- Based on this Spectracom can commit to a drift rate of  $5 \times 10^{-12}$  per month provided
  - A. The unit is initially synchronized to GPS for a minimum of 2 weeks
  - B. The unit isn't powered off after it was synchronized.

**Email from Dick Fox (6/10/12) to TOYO** "Our design team is telling me the rubidium needs 2 weeks of GPS disciplining to settle"

---

## **\*\*Show clock page (System date/time display in the browser)**

- Provides ability to display date, time and sync status
- Version 5.2.1: Updated Show Clock page to improve clock and system status info displays. V5.2.1 also added a "Home" button to get back to the Home page of the browser.

---

## **\*\*SMPTE Time code (LTC and VITC)**

- We don't support SMPTE with any of our products, as of at least Oct 2019.

**Question from Danny Loke: ... "the NTP servers will require an additional LTC or VITC input card module"**

**Reply from Keith (23 July 15)** I don't recall ever hearing the terms of LTC or VITC, so a quick Google search to see what these terms mean in the CCTV/video realm provided me with a term I have run across a couple of times (very rarely). This word is "SMPTE". SMPTE stands for Society of Motion Picture And Television Engineers. What these two terms are referring to is also referred to as "SMPTE time code". This is a very unique time code for synchronization of a very specific application.

LTC is "Longitudinal time code" and VITC is "Vertical Time Code". For more info on what these are and the differences between them, refer to <http://www.filmunderground.com/34/kb/NWFS/lc-vs.-vitc.htm>.

We don't currently provide any support for SMPTE time code. It's a very seldom requested capability, so it hasn't been beneficial to us to add support to our products for it. But this is not to say we wouldn't do it for the appropriate size order that would justify all the costs associated with the development. I highly doubt we could justify it with the purchase of a SecureSync. But if there is significant potential with your customer, Josh can with our Senior Product Manager to see what it would take for us to add it, whether it's based on the quantity of units they would be ordering, or perhaps through NRE fees. But if they are looking at just one or two units for example and require this capability, unfortunately we won't likely be able to help them, (they will need to "look elsewhere" to meet their requirements).

If you feel there is significant potential with this customer, if the SecureSync was able to provide SMPTE time code, work with Josh for more details on what would be required for us to consider it!!



---

## Logs/Syslog

- Refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Alarms and logs](#)
- And in the SecureSync online manual:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/OPRTN/Logs\\_Remote%20Servers.htm?Highlight=syslog](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/Logs_Remote%20Servers.htm?Highlight=syslog)
- Supports Syslog capability (sending logs to a remote Syslog server on the network).
- All SecureSync Logs are stored in the home/spectracom/log directory.

### A) Syslog (Remote logs/remote logging)

- Example freeware Syslog server software:
  - “Event Log Analyzer” <https://www.manageengine.com/products/eventlog/download-free.html>
  - “Syslog server 1.2.3” (<http://www.softpedia.com/get/System/System-Miscellaneous/Syslog-Server.shtml>)

#### Free Syslog software for Windows:

More recently (Jan 2018) I downloaded/installed “Event Log Analyzer”

- I downloaded/installed “Syslog Server 1.2.3” .
  - Refer to <!:Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Syslog>

---

### rsyslog (or syslog-ng)

- These are alternate syslog packages, we are not using either of these, in at least versions 5.8.1 and below
- we may need to switch to one of these for enhanced capabilities
  - Refer [JIRA] (SSS-478) Raytheon is requesting syslog messages (log entries) to have milliseconds precision (per Salesforce case 162730)

---

### Syslog Protocol

#### RFCs for Syslog protocol

- Our syslog operation follows RFCs 3164 (obsolete) and 5424 <https://tools.ietf.org/html/rfc5424> and [http://www.rfc-editor.org/search/rfc\\_search\\_detail.php?rfc=3164&pubstatus%5B%5D=Any](http://www.rfc-editor.org/search/rfc_search_detail.php?rfc=3164&pubstatus%5B%5D=Any)
- Cisco site with great info on the Syslog Protocol: <http://www.ciscopress.com/articles/article.asp?p=426638>
- Contains info on Facility and Severity codes, Timestamp and message formats, etc

## Syslog header (RFC 5424) vs syslog-ng header (RFC 5424)

Refer to: <https://success.alienvault.com/s/article/difference-between-Syslog-and-Syslog-NG>

### 1. Example Syslog packet

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
```

### 2. An example syslog-ng packet:

```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com evntslg - ID47 [exampleSDID@32473 iut="3" eventSource= "Application" eventId="1011"] BOMAn application event log entry
```

## Time/date/year info in syslog messages

**Note:** We use syslog format (not syslog-ng/rsyslog which uses a different header than syslog)

- UTC time only (never local)
- No year info

### Example Syslog packet

```
Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick
```

---

## Syslog messages/ UDP port number

### SSL/TLS Encryption of logs being sent to Syslog servers/Desire to support TLS encryption

- Refer to Salesforce Cases such as 190596
- Refer to JIRA ticket SSS-625
- As of at least versions 5.8.4 and below, Syslog entries are sent in the clear (our syslog does not use SSL)

The messages do not use SSL for encryption of the entries:

- **“Local Logging”**: You can individually configure which log files get saved in the box (**Management -> Logs** page, in each log tab).
- **“Remote Logging”**: You can individually configure which log files get sent to Syslog (**Management -> Logs** page, in each log tab)

---

## SecureSync sends Syslog messages as UDP on port 514

### UDP/Port Number

- Uses **UDP port 514** (hard-set in software versions prior to 5.7.1).
- A) v5.7.1 and above (starting 6 Sept 17)** now allow the port to be custom-configured.
  - From 5.7.1 release notes: **“Syslog Port Number can be changed in web ui.”**

## B) Versions 5.7.0 and below, port is hard-set and can only be changed via a patch update.

Q Can syslog send logs via TCP instead of UDP

A Syslog sends logs via UDP port 514. Syslog in the SecureSync isn't able to send logs via TCP.

FYI Syslog in the SecureSync follows RFCs 3164 and 5424. The following statement is from RFC 3164 (<https://www.ietf.org/rfc/rfc3164.txt>)

Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514."

- Special Patch Ron Dries created for Les Ulis customer to change the port to 700 instead of 514 (now a standard configuration in versions 5.7.1 and above, per ECO-1338, 6 Sept 17)

This special patch for versions 5.7.0 and below is now included in versions 5.7.1 and above (starting 6 Sept 17)

**From 5.7.1 release notes: "Syslog Port Number can be changed in web ui."**

**Email from Ron Dries to Sylvain (11 Nov 16)** I created a patch for SecureSync that can be applied to a SecureSync with software version 5. It changes syslog to use port 700 instead of 514. The patch image and md5 sum are released to design in Arena part number 1200-SU02-5XXS

Yes the patch will need to be applied each time the SecureSync is updated. However, it will persist after a **reboot/shutdown**. The patch can be applied to any 5.X.X version of software.

"In the event that a syslog server does not support listening on the standard syslog port, you may redirect the syslog port to the desired port by utilizing built-in port forwarding capability in network switches (search online for port forwarding or port mapping)."

---

### Identifying in a syslog server which SecureSync sent a log entry

- Each log entries contain the DNS Hostname of the SecureSync.

**Note (Oct 31, 2012):** versions 4.8.7 and below were found to be sending a hard-coded "Spectracom" as the Hostname, even if the hostname is no longer this default value. So even if the hostname has been changed, the hostname will still be reported as "Spectracom". This is supposed to be fixed in the next software release.

- **Email from Dave Sohn (11/1/12)** How the syslog server application resolves the messages it receives to inform the user of the host's information is separate. The program I used is trying to resolve the IP address of the unit it received the message from based on several factors. If it fails to resolve to something better, it simply reports the IP address. Their syslog server may do it differently, or they want it in the message itself.

---

### Configuration of syslog

#### IPv6 for Syslog

- Refer to Mantis case 1897

**Mantis cases 1849/1897:** Syslog not working with IPv6 addresses.

**Status update per Dave Sohn (8 Mar 2013):** "Our current syslog package does not support IPv6. Either a new package/version or patch are required. (This is recorded in Mantis case 1897)

- 
- Refer to syslog tech notes for SecureSync and 9400s
    - **SecureSync:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Syslog>
    - **9400 series:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\Syslog>

**A) Classic interface browser:**

- Configured in each log of the *Setup* -> *Logs* page of the browser

**B) Newer browser:**

- Configured in each log of the *Management* -> *Log Configuration* page of the browser

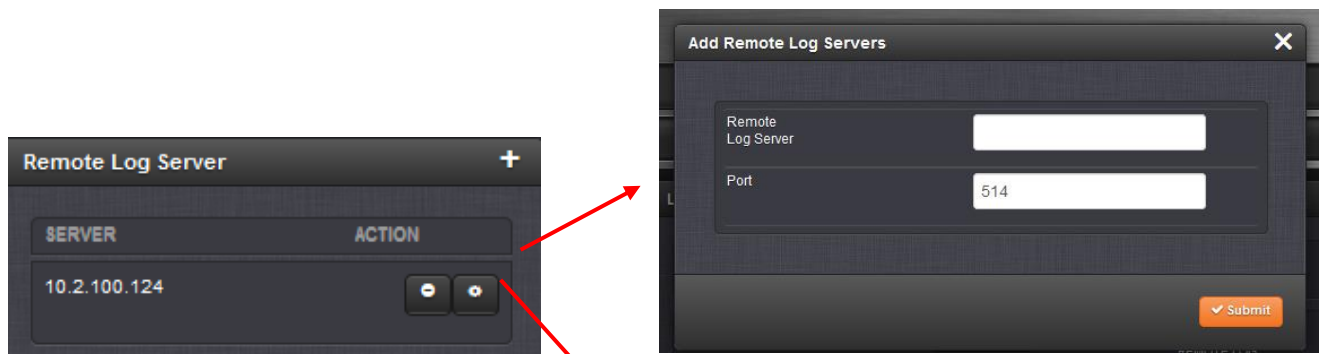
**Ability to reset Syslog settings only back to default** (added in update v5.7.1)

**Ability to configure the Syslog port number** (added in update v5.7.1)

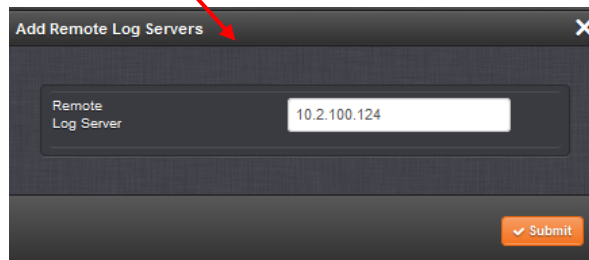
**Note:** Keith confirmed the Main default gateway does not need to be properly configured for syslog to still work.

**Step 1: Add up to 8 Remote log Server (s) (left side of the Log Configuration page)**

**(Versions 5.7.1 and above)**



**(Versions 5.7.0 and below)**



**Step 2: Add Remote log Server (s) to each Log type (such as Events, Alarms Auth, etc) in the list of logs in the Management -> Log Configuration page**

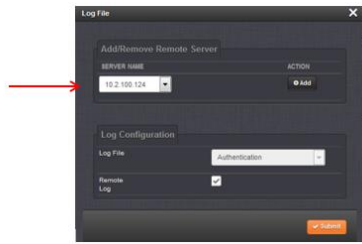
**NOTE:** due to ability to individually configure each log type to be able to be sent to different log servers, the user MUST individually “add” the syslog server for each log type.

1. Press the middle of the three icons for each log type desired to be sent to Syslog server(s)
2. Select the desired Syslog address in the drop-down.
3. Press the “Add” button on the right-side of the pop-up window and Submit. This sets the Server name/address.
4. If more than one syslog server was added in step 1, the drop-down list will continue to be present listing all of the other available syslog servers available to send this particular log to

**Note:** Make sure the “Remote Log” checkbox at the bottom of the window is selected.

**Example:**

A) Before pressing “add” (must be done for each log type)



B) After pressing “add”



C) If more than one syslog server was added to the list on the main log config page (allows this log to be sent to up to eight different syslog servers)



**Ability to reset just the syslog configuration**

**Update version 5.7.1 (starting 6 Sept 17) and above now provide ability to delete just the syslog configuration.**

- From 5.7.1 release notes: “Corrected ability to restore Syslog to default configuration”

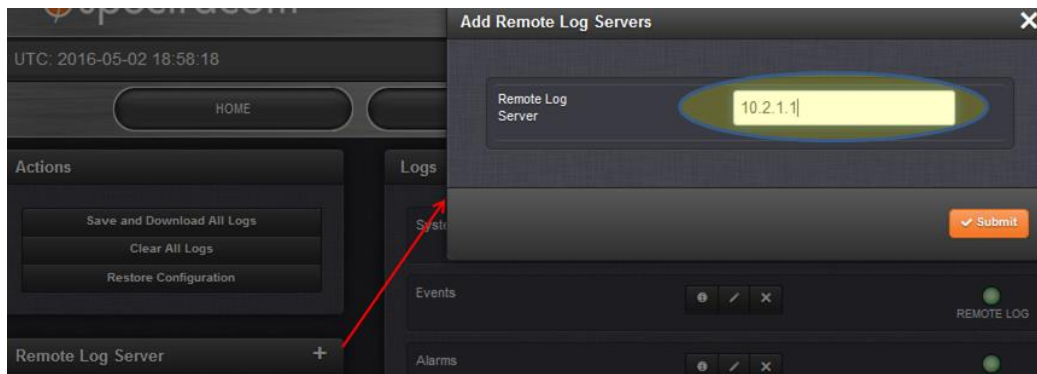
**Syslog server(s) are configured for each log in the browser**

**Email from Keith on how to configure syslog**

All of the logs that can be viewed in the web browser can also be sent to a syslog server. Below is info on how to configure the logs to be sent to a syslog server.

First, add the desired syslog server(s) to the list of available syslog servers that each log type can be individually configured to be sent to (overall, multiple syslog servers can be listed, with each log file type being able to be sent to any one of the servers in this list).

On the left side of the **Management -> Log Configuration** page of the browser, press the “+” sign to the right of “**Remote log Server**”. In the pop-up window, enter the IP address of the syslog server and Submit. Repeat as desired to enter additional.



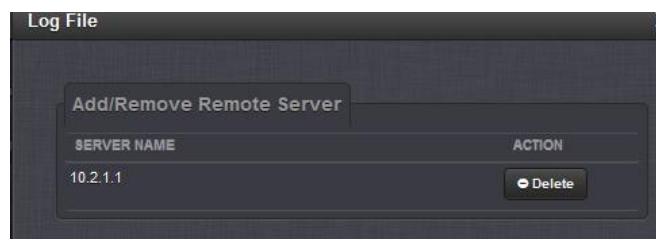
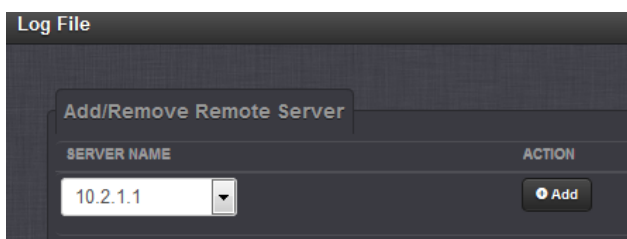
Because the log files can be individually configured as to which remote server it's entries are sent to, each log file type (such as the System Log for example) has to be individually configured to be sent to the desired remote server, before its logs will be sent to any remote server. You need to add (select) a Remote server from the list of previously added to "Remote Log servers" (on the left side of Log Configuration page).

To configure a remote sever to each log type (this can't be done as a single global setting for all of the log files), after adding one or more remote server addresses to the list (on the left side of the page) press the same middle icon (**Management -> Log configuration** page of the browser) for each log type you wish to send to a remote server, you need to add (select) one or more Remote servers, as previously added to the list of "Remote Log servers" on the left side of this page.

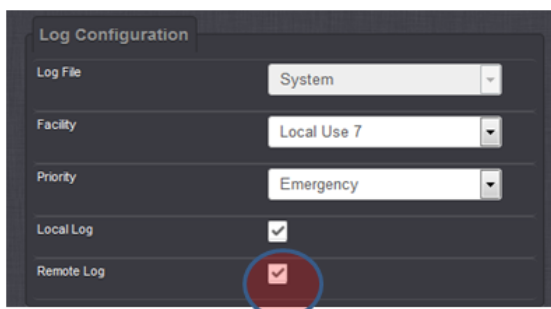
Each log of the SecureSync has its own remote logging enable checkbox that also needs to be selected, if you desire for that file's log entries to be sent to a specified syslog server.

The remote logging enable for each log file/type (such as the "Qualification" log for instance) is in the **Management -> Log configuration** page of the browser. For each log file you wish for its logs to be sent to remote servers, click the middle of the three ICONS (the pencil ICON) for that log file. In the **server name**" drop-down of the pop-up window, select the particular syslog server you wish to send this log file to and then press the Add button.

The "Add" button and the "Server name" drop-down field will vanish after pressing the Add button



Make sure "Remote Log" checkbox is selected (it is selected for all log files by Factory default". But if it's been since unchecked, its log entries won't be sent to a remote server.



**Local log:** When selected, causes log entries for this log file to be stored inside the time server. If its unselected, logs for this file will not be stored within the time server

**Important Note:** Please be aware that the specific combination of the **Facility** and **Severity** codes for each log file (as also configured in the same pop-up window mentioned above) define where the Log entries are actually sent to in the SecureSync/syslog server. Changing any of these two values will result in the particular log entries that are supposed to be sent to one Log file actually being sent to another Log file. So log files can become inter-mixed inside the SecureSync, making it nearly impossible to review them in the browser, the CLI or if the logs are downloaded from the unit. For this reason, we do not recommend any of the facility and Severity codes be changed from the default settings.

### Troubleshooting suggestions:

- Make sure each individual log file has been configured with a syslog server address (*Management* -> *Log Configuration* page of the black/charcoal browser)
- Login to the CLI interface (telnet or ssh connection) and verify if you can ping the Syslog server.
  - Check the main default port/gateway in the configured correctly (*Management* -> *General Setup* page of the black/charcoal browser)
  - Perform a wireshark or tcpdump capture on the SecureSync's switch to see if syslog packets are being sent.
  - Verify the syslog server is listening on syslog port 514 and there are no firewalls in between that may be blocking this port.

**Storage of Syslog configs/remote server IPv4 addresses : desire to script the adding of remote servers.**

#### A) Earlier software versions having mysql database (prior to switching to sqlite database)

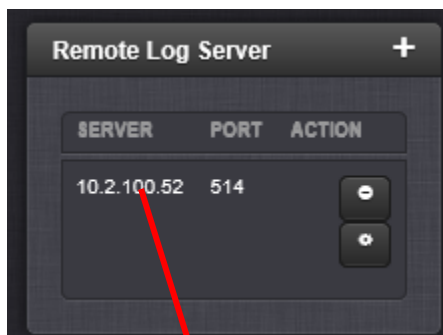
**(Modified) Email from Dave Sohn (7 Jan 16) about where the Syslog Servers are stored** They are stored in /etc/syslog.conf, but also in the SQL (or MySQL for older SW) databases.

**Email from Ron (7 Jan 16)** We store syslog servers in the MySQL database and then they are written into the configuration files. I'm also not sure if a customer would have permissions sufficient enough to run a script and add that information in.

At the current 5.3.1 there is a bug that prevents new servers from being added, however there is a patch that I have worked on that addresses the issue. I have not released the patch yet.

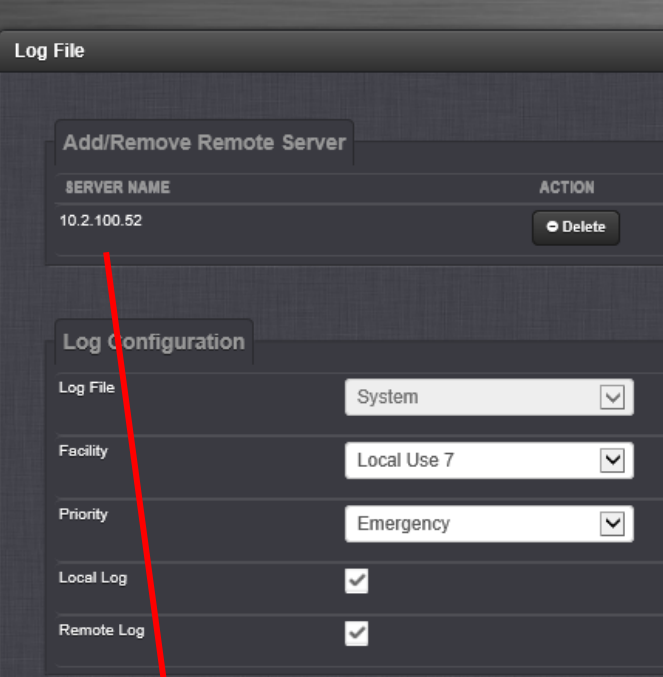
#### B) More recent software versions (having sqlite database instead of earlier mysql database (like 5.7.1 and above???)

- Syslog server address(es) is still stored in /etc/syslog.conf, and now also stored in the sqlite dbase (home/spectracom/config/backup.sql.tar.gz file in the config backup bundle).



home/spectracom/config/backup.sql.tar.gz file in the backup config bundle

```
backup.sql
6269 ~ primary key autoincrement,
6270 boolean NOT NULL,
6271 DEFAULT NULL);
6272 ethernet_ui_banners VALUES(1,0, '');
6273 NOT EXISTS "remote_servers" (
6274 ~ primary key autoincrement,
6275 char(255) NOT NULL,
6276 boolean DEFAULT '0' NOT NULL,
6277 boolean DEFAULT '0' NOT NULL,
6278 boolean DEFAULT '0' NOT NULL,
6279 boolean DEFAULT '0' NOT NULL,
6280 boolean DEFAULT '0' NOT NULL,
6281 boolean DEFAULT '0' NOT NULL,
6282 boolean DEFAULT '0' NOT NULL,
6283 boolean DEFAULT '0' NOT NULL,
6284 boolean DEFAULT '0' NOT NULL);
6285 remote_servers VALUES(1, '10.2.100.52', 1, 0, 0, 0, 0, 0, 0, 0);
6286 NOT EXISTS "preferences" (
6287 ~ primary key autoincrement,
```



etc/syslog.conf file in the backup config bundle

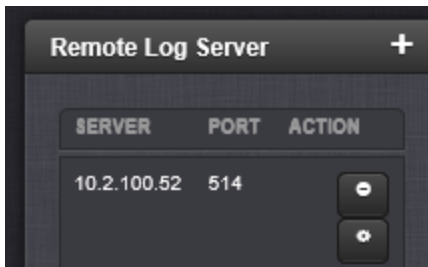


```
syslog.conf
1 auth,authpriv.* /home/spectracom/log/auth.log
2 *.*;local1,local2,local3,local4,local5,local6,local7,auth,authpriv,daemon,kern,mail,user,c
  /home/spectracom/log/sys.log
3 daemon.notice /home/spectracom/log/daemon.log
4 kern.* /home/spectracom/log/kern.log
5 mail.* /home/spectracom/log/mail.log
6 user.* /home/spectracom/log/user.log
7 cron.* /home/spectracom/log/cron.log
8 local6.* /home/spectracom/log/ntp.log
9
10 Spectracom application specific entries
11 local7.=emerg /home/spectracom/log/system.log
12 local7.=emerg @10.2.100.52
13 local7.=alert /home/spectracom/log/events.log
14 local7.=alert @NULL
15 local7.=alert @NULL
16 local7.=alert @NULL
17 local7.=alert @NULL
18 local7.=alert @NULL
19 local7.=crit /home/spectracom/log/alarms.log
20 local7.=crit @NULL
21 local7.=crit @NULL
22 local7.=crit @NULL
23 local7.=crit @NULL
24 local7.=crit @NULL
25 local7.=err /home/spectracom/log/timing.log
26 local7.=err @NULL
27 local7.=err @NULL
28
```

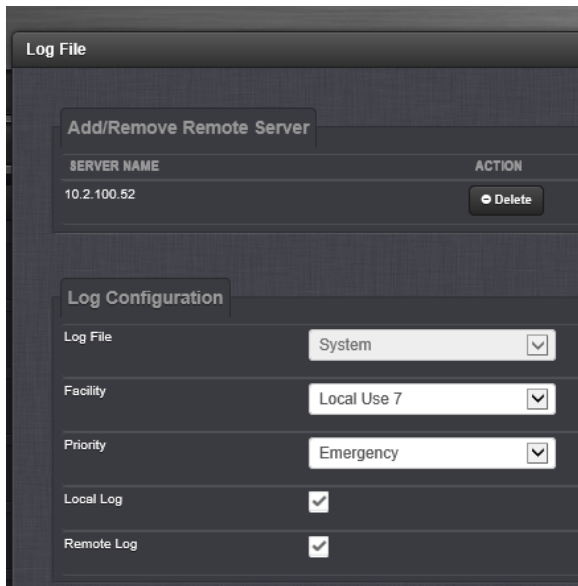
**Email Keith sent (31 July 2019)** Also referencing your original email, there are a few configs that are stored in an sqlite database, instead of the standard config files. I haven't "confirmed" this with the Engineers yet, but I personally found that the syslog server address(is) is stored in both the etc/syslog.conf file, as well as in the "remote\_servers" table of this database.

From what I see/suspect:

- 1) The sqlite database stores the entire list (of one or more) of the desired syslog servers (which are then displayed in the drop-down remote server field, to be able to select the desired server for each individual log file type) as shown below:



- 1) ...While the etc/syslog.conf file stores all the individual log file configurations (such as the selected syslog server for the "System log", for example, as shown towards the top of the screenshot below),,,



In order to restore all syslog server configs, I believe both the etc/syslog.conf file, and at least the syslog server values in the sqlite database, need to be restored,

Will get back to you with additional info on syslog v6 support and syslog restore configuration, once I hear back from the SecureSync Product Manager.

---

## Operation/Software Issues with Syslog

### 1) (found in v5.9.4) NTP “Remote Log Server” field is blank, but the node succeed to send logs to remote log server

- Refer to Salesforce Case 283695/JIRA SSS-1263
- Kobe Zhang with PayPal reported the following for v5.9.4 SecureSync: “We found out NTP “Remote Log Server” field is blank, but the node succeed to send logs to remote log server,”

### 2) Authentication log’s “Remote Log” checkbox cannot be unselected (and it doesn’t have a checkbox displayed to disable its “Local Log” (observed in v5.8.4)

- Refer to Salesforce Case 203334
- Refer to JIRA ticket SSS-661

### 3) V5.3.1: Can’t enter any new Remote Log server addresses (left side of the Management -> Log Configuration page of the browser)

- Refer to Mantis case 3195
- When trying to add a new syslog server, reports error message “500: Interval Server Error”
- If updated to version 5.3.1, previously entered syslog server addresses are carried forward and not an issue. This issue just affects new units shipped at 5.3.1 or units that happened to be cleaned with v5.3.1 installed.
- Planned to be addressed in v5.4.0 update, ~end of Jan 2016.

#### 4) Syslog configurations not being backed-up/cloned (observed in 5.3.0)

- Reported in Version 5.3.0
- Refer to Mantis case 3161
- Refer to Salesforce case 19768

Trevor Bannard with Janes street reported syslog configs not being backed-up:

when I save the config and upload it to another device, the log configuration does not seem to be applied to the new device (the remote log server is not present in the log configuration on the new device, and likewise each log component doesn't have the log server). When I perform the 'Upload configuration' function it works for a few seconds, then returns to the upgrade/backup screen."

#### 5) NTP and Auth logs not configurable/can't be sent to Syslog

##### Update Versions

- Version 5.1.2 added ability for Auth (Authentication) logs to be sent to Syslog servers.
- As of at least versions 5.2.0 and below, the NTP log entries can't be sent to a syslog server.
- Refer to Mantis case 1775
  - As of at least versions 5.0.1 and below, both the NTP and Auth (Authentication) logs are not currently configurable (they are not currently listed in the Setup -> Logs page of the browser). There are no Facility/Priority codes associated with them and they have no place to configure them to be sent to a Syslog

---

#### Verification that Syslog is working / Troubleshooting Syslog not working

- Verify port
- Use Syslog software to verify log entries are being received.
- Use tcpdump in the SecureSync to verify "syslog" packets are being sent
- Use Wireshark to capture "syslog" packets are present.
- Review the **/etc/syslog.conf** file (using cli interface or via config bundle)

##### **example cat of the etc/syslog.conf below is from version 5.7B software**

**Note:** In this example below, the System log is the only Log file thus far to have a Syslog server added to it, from the list of available Syslog servers (as shown with the entry of "@10.1.2.3")

```
spadmin@Spectracom /etc $ cat syslog.conf
auth,authpriv.* /home/spectracom/log/auth.log
*.*:local1,local2,local3,local4,local5,local6,local7,auth,authpriv,daemon,kern,mail,user,cron.none /home/spectracom/log/sys.log
daemon.notice /home/spectracom/log/daemon.log
kern.* /home/spectracom/log/kern.log
mail.* /home/spectracom/log/mail.log
user.* /home/spectracom/log/user.log
cron.* /home/spectracom/log/cron.log
local6.* /home/spectracom/log/ntp.log

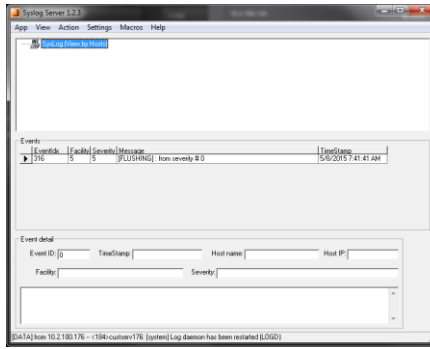
# Spectracom application specific entries
local7.=emerg /home/spectracom/log/system.log
local7.=emerg @10.1.2.3
local7.=alert /home/spectracom/log/events.log
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=crit /home/spectracom/log/alarms.log
local7.=crit @NULL
```

```
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
local7.=err -/home/spectracom/log/timing.log
local7.=err @NULL
local7.=err @NULL
local7.=err @NULL
local7.=err @NULL
local7.=err @NULL
local7.=warn -/home/spectracom/log/qual.log
local7.=warn @NULL
local7.=warn @NULL
local7.=warn @NULL
local7.=warn @NULL
local7.=warn @NULL
local7.=debug -/home/spectracom/log/osc.log
local7.=debug @NULL
local7.=debug @NULL
local7.=debug @NULL
local7.=debug @NULL
local7.=debug @NULL
local7.=notice -/home/spectracom/log/journal.log
local7.=notice @NULL
local7.=notice @NULL
local7.=notice @NULL
local7.=notice @NULL
local7.=notice @NULL
local7.=info -/home/spectracom/log/update.log
local7.=info @NULL
local7.=info @NULL
local7.=info @NULL
local7.=info @NULL
local7.=info @NULL
```

```
Spectracom application specific entries
ocal7.=emerg -/home/spectracom/log/system.log
ocal7.=emerg @10.1.2.3
ocal7.=alert -/home/spectracom/log/events.log
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=crit -/home/spectracom/log/alarms.log
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=err -/home/spectracom/log/timing.log
ocal7.=err @NULL
ocal7.=err @NULL
```

---

**Free Syslog software for Windows:** I downloaded/installed "Syslog Server 1.2.3" . Refer to [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Syslog](#)



## TCPdump capture of syslog messages being sent

**Note:** the screenshot below shows tcpdump listening on port 514 of all Ethernet interfaces (filtering for port 514 will only capture syslog messages being sent). This screenshot from v5.3.0 software shows the two separate journal log entries I caused to be sent by changing web browser configs.

```

0 packets dropped by kernel
spadmin@CustService-177 ~ $ tcpdump port 514
-bash: /usr/sbin/tcpdump: Permission denied
spadmin@CustService-177 ~ $ sudo tcpdump port 514
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:05:39.526873 IP 10.2.100.177.syslog > 10.2.100.124.syslog: SYSLOG local7.notice, length: 145
19:06:25.958868 IP 10.2.100.177.syslog > 10.2.100.124.syslog: SYSLOG local7.notice, length: 113

```

## Associated Journal log entries that were asserted during this test.

```

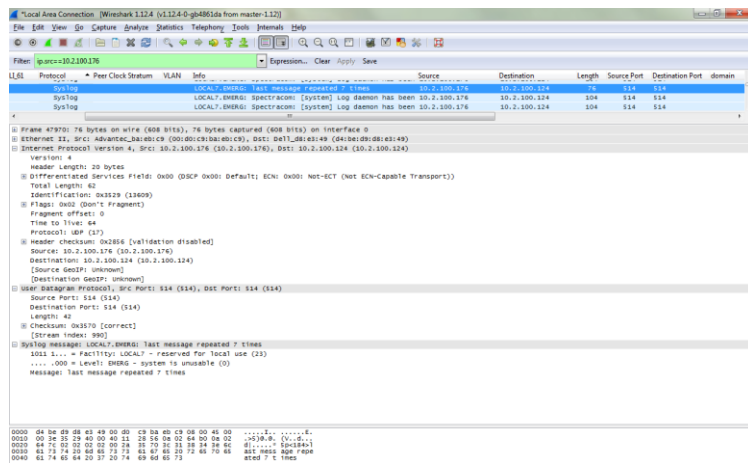
TZ: -18000
Nov 5 18:37:11 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
from Time Scale: UTC to Time Scale: TAI
Nov 5 18:37:31 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
from Time Scale: TAI to Time Scale: UTC
Nov 5 18:37:50 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for GPS: 18
Nov 5 18:37:52 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for TAI: 37
Nov 5 18:38:12 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for GPS: 17
Nov 5 18:38:14 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for TAI: 36
Nov 5 19:05:39 CustService-177 CustService-177: [webui] Changed Format for Display Output 0 i
slot 0 from DP (0) Format: (1) 24-hour to DP (0) Format: (0) 12-hour
Nov 5 19:06:25 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
from Time Scale: UTC to Time Scale: TAI
spadmin@CustService-177 /home/spectracom/log $

```

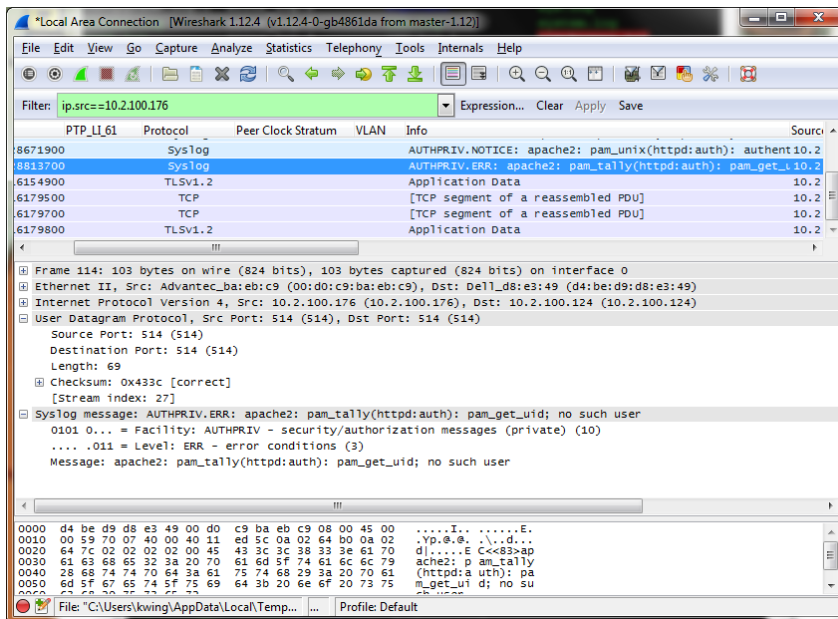
## Wireshark capture of syslog entries

Example filter can use: `ip.src==10.2.100.176 and udp.port==514`

*Example Syslog packet capture*



## Example capture of an Auth log entry being sent to syslog due to trying to login with invalid credentials



### Syslog log in the unit (sys.log)

- There is no syslog log available in the web browser.
  - Sys.log can only be viewed via the CLI. It's in the **home/spectracom/logs** directory
- Contains entries for syslog stopping and starting

### A) Logs not present in the syslog server

- Verify the syslog configs are correct (**Management -> Log Configuration** page of the newer browser)
- Check main default port/gateway is correct (**Management -> General Setup** page of the newer browser)
- Login to cli interface and try pinging out/traceroute CLI command to the syslog server (could be a network issue)

---

## Logs

### FAQS about SecureSync Logs

Q. If I delete all the log files, does the SecureSync **automatically** generate new ones from scratch?

A. **Keith's response: Absolutely. New log files will automatically start to be created, after they have been deleted.**

Q. How often does the system update the log entries of the file when an "event" happens?

A. **Log entries are asserted into the logs each time an event occurs and each time the event clears. No log entries are added in between the event occurring and the events clearing.**

### Timestamp formats for syslog standards

- Refer to sites such as: <http://www.ciscopress.com/articles/article.asp?p=426638>
- The Syslog standard for timestamps (MMM DD HH:MM:SS) doesn't include the current year or any digits for milliseconds.

### Log requirements for PCI-DSS/ PCI compliance

- refer to (in this doc): [PCI-DSS/ PCI compliance](#)

---

### Missing expected log entries/"Search" field for the logs (top right of the individual log pages)

- Using the Search field in each log page to filter for only certain log entries can cause expected log entries not to be displayed in the browser, even though they do exist
- The Search field considers a space to be the start of another separate filter, instead of being part of the entire string ("Jul 07" searches for entries containing both "Jul" and "07", not just for entries containing the string of "Jul 07").

The Search field considers a "space" as the beginning of another filter (it doesn't search verbatim for the text and space in between. It considers one space as two separate filters. Two spaces will result in three separate filters, etc),

For example, using the search of "**Jul 07**" won't find only log entries that were asserted on Jul 7<sup>th</sup>. Instead, it finds all entries that contain both "Jul" and "07" somewhere in the whole log entry. So it may show log entries for Jul 25<sup>th</sup>, just because the data in those entries also contains an "07" somewhere in the entry. It doesn't search for "Jul 07" as-is to just display entries for the 7<sup>th</sup>.

This can cause confusion, because using a search may result in expected logs not being displayed in the browser, though the entries were actually asserted the full log file in the background.

---

### Year value is not included in log entries

- Because we have to use Syslog formatting (as we can send logs to syslog servers) and because Syslog itself does not contain year information, unfortunately our logs can't contain year information.

---

### "Happy New Year" log messages to indicate present year in the logs

- Added to all of our log files at the first of the year, starting in software version 5.3.1, to indicate New Year rollover has occurred.

Q. Logs – Year stamp on the logs. Could this be suggested to engineering for consideration in a later release?

A. **Keith's response: The logs are in Syslog format as needed, because the product has the ability to send log entries to Syslog servers. Unfortunately, Syslog format does not include year information (not a Spectracom decision or design). We have discussed this with engineering already, and unfortunately, the year cannot be added to the logs (I also wish it could).**

## Potential issue with the “Happy New Year”: message stopping to be asserted on 1 January

- Observed with “simulated” year rollover testing, with 5.8.9 installed.
- Refer to JIRA Ticket

## Other ways to tell the “present year value”, without using the “Happy New Year” log entry (such as for year rollover)

- Per Keith- after “scouring” a logs bundle, I found a few “OK” ways to also tell the year incremented correctly after 1 January New Year rollover (refer to Salesforce Case 256666). Excerpt from email I sent for this case is below”:

1. **Manifest log** (time/date of every reboot. Entries include the current year value)
2. Per the **NTP log** on 12 January, "0.0.0.0 c41c 0c clock\_step -31654799.998135 s". This entry, indicating a very large time correct to NTP equates to a 366 day (one year) time correction. This huge time change was to account for the year changing from 2020 to 2021.
3. Per the **Apache Web browser error logs** (the first data entry below is just before the SecureSync was halted on 18 December, and the next sequential entry in the log was after it was booted back up again, on 12 January:

[Fri Dec 18 07:11:27 2020] [notice] caught SIGTERM, shutting down  
Failed loading /u

...

[Tue Jan 12 17:10:12 2021] [notice] Apache/2.2.34 (Unix) DAV/2 mod\_ssl/2.2.34 OpenSSL/1.0.2o configured --  
resuming normal operations  
Failed loading /usr/lib/php5.5/lib/[opcache.so](#):...

My testing, and the log entries above, show that the SecureSync will (and did) automatically increment the present year (2020 to 2021), with the transition from 31 December to 1 January, with IRIG input having no year value present

---

## Log entries are in UTC time scale

**Note:** Log entries can't be configured for local time scale. They are always in UTC time scale.

Q. Also in the logs section can you define that the log stamp use a local time stamp as opposed to just taking the time based on the UTC time input to the SecureSync?

**A. (based on an email from Dave Sohn 8/24/12)** The logs are always in the UTC time scale. There is no way to configure the time stamps to be in Local time scale. We use syslog for our logging mechanism. The timestamps are provided by it and use the kernel time, which is in UTC time scale.

---

## Reporting of Model and version in the logs/log capture

- **Version 5.2.1 update** (Apr 2015) added Model and Serial Number to the System Log at each start-up.
- **Version 5.2.0 update** started adding the software version to the log capture



## \*\*Ability to view the logs (log entries) with CLI interface

1. Login with either telnet or ssh.
2. Type **cd log** <enter> to change to the log directory
3. Type **ls** <enter> to list all logs.

```
spadmin@Spectracom ~/log $ ls
alarms.log          cron.log.3        events.log.1      ntpstats         rexd.log          sys.log.2
alarms.log.1       cron.log.4        events.log.2      osc.log          snmpd.log         sys.log.3
alarms.log.2       daemon.log        events.log.3      osc.log.1        snmpd.log.1      sys.log.4
alarms.log.3       daemon.log.1      events.log.4      osc.log.2        snmpd.log.2      system.log
alarms.log.4       daemon.log.2      journal.log       osc.log.3        snmpd.log.3      timing.log
auth.log           daemon.log.3      kern.log          osc.log.4        snmpd.log.4      update.log
```

4. To view the log entries, type **cat** <enter> followed by the name of the log (Example: type **cat auth.log** <enter>) to view the Authentication log entries.

```
-bash: cd: log: No such file or directory
spadmin@Spectracom ~/log $ cat auth.log
```

## \*\*Ability to delete the logs

### A) Ability to delete the logs via CLI

**Note:** The **clearlogs** command only clears the logs that are displayed in the browser (such as Qual, NTP, etc). This function does not clear the “system” logs in the background only (such as sys.log, daemon.log, kern.log, mail.log, rexd.log, cron.log, mysql\_create.log and system.log)

- Can't delete the NTP logs via CLI before version 5.1.5???
- I believe version 5.1.5 introduced the **clearlogs** CLI command to clear logs.

### B) Ability to delete the logs via the newer web browser

- Two different locations to delete the logs:

5. Delete just the logs that are displayed in the web browser (Alarms, Events, NTP, etc) (not the logs in the background, such as kern.log, sys.log, etc)

**Management -> Log Configuration page**, click the “**Clear All Logs**” button in the upper-left corner).

6. Delete all of the logs (the ones in the background and the ones in the browser)

Via the bottom-left corner of the **Tools -> Upgrade/Backup page** (click the “**Clear All Logs**” button).

**Note:** The **clearlogs** command only clears the logs that are displayed in the browser (such as Qual, NTP, etc). This function does not clear the “system” logs in the background only (such as sys.log, daemon.log, kern.log, mail.log, rexd.log, cron.log, mysql\_create.log and system.log)??

**Update to Note above:** Update versions 5.4.5 and above now deletes the Auth and NTP logs.

### Software issue associated with deleting logs and NTP stats via the browser

- With at least software version 5.2.1, the “Clear All logs” button.
- Note the associated CLI command work fine in both Models.

- Refer to Mantis case 3049. <http://cvsmantis.int.rolia.com/mantis/view.php?id=3049>
- Fixed in version 5.3.0 (Sept 2015)

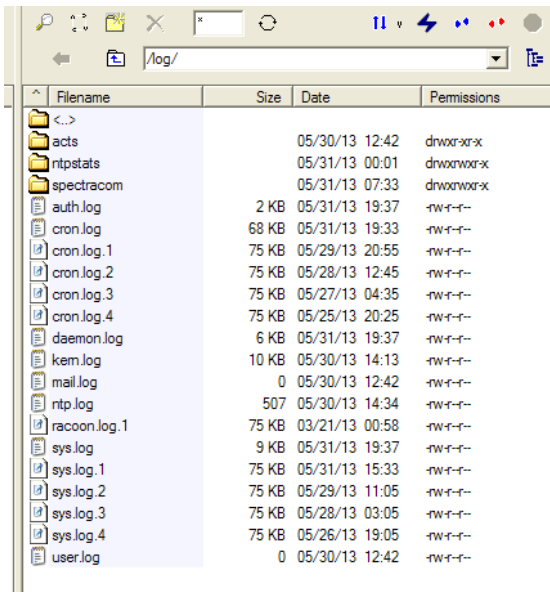
---

## Log file sizes/Log rotation

- View all of the logs via telnet/ssh
  1. Log in with telnet/ssh
  2. Issue an **ls -al /home/spectracom/log** command to view log sizes. (Note: This command doesn't report log sizes).
  3. Go to the **log** directory.

## Current size of all log files can be viewed

1. Log in with FTP/SCP
2. Issue a **ls -al /home/spectracom/log** command to view log sizes. (Note: This command also works with telnet to list the logs. But it doesn't report log sizes).
3. go to the **log** directory.



| Filename      | Size  | Date           | Permissions |
|---------------|-------|----------------|-------------|
| <.>           |       |                |             |
| acts          |       | 05/30/13 12:42 | drwxr-xr-x  |
| ntpstats      |       | 05/31/13 00:01 | drwxrwxr-x  |
| spectracom    |       | 05/31/13 07:33 | drwxrwxr-x  |
| auth.log      | 2 KB  | 05/31/13 19:37 | -rw-r--r-   |
| cron.log      | 68 KB | 05/31/13 19:33 | -rw-r--r-   |
| cron.log.1    | 75 KB | 05/29/13 20:55 | -rw-r--r-   |
| cron.log.2    | 75 KB | 05/28/13 12:45 | -rw-r--r-   |
| cron.log.3    | 75 KB | 05/27/13 04:35 | -rw-r--r-   |
| cron.log.4    | 75 KB | 05/25/13 20:25 | -rw-r--r-   |
| daemon.log    | 6 KB  | 05/31/13 19:37 | -rw-r--r-   |
| kern.log      | 10 KB | 05/30/13 14:13 | -rw-r--r-   |
| mail.log      | 0     | 05/30/13 12:42 | -rw-r--r-   |
| ntp.log       | 507   | 05/30/13 14:34 | -rw-r--r-   |
| racoona.log.1 | 75 KB | 03/21/13 00:58 | -rw-r--r-   |
| sys.log       | 9 KB  | 05/31/13 19:37 | -rw-r--r-   |
| sys.log.1     | 75 KB | 05/31/13 15:33 | -rw-r--r-   |
| sys.log.2     | 75 KB | 05/29/13 11:05 | -rw-r--r-   |
| sys.log.3     | 75 KB | 05/28/13 03:05 | -rw-r--r-   |
| sys.log.4     | 75 KB | 05/26/13 19:05 | -rw-r--r-   |
| user.log      | 0     | 05/30/13 12:42 | -rw-r--r-   |

---

## Issues associated with all or individual logs

### 1) Only the Journal log can't open in browser (all others open fine and it can be viewed in CLI)

- Observed in v5.8.5
- Refer to Salesforce Case 208320 and JIRA ticket SSS-687
- Appears to be due to erratic characters in Journal log, after editing network settings via the front panel

### 2) Logs not rotated in software versions 5.8.0 and 5.8.1

- Known issue fixed starting in v5.8.2

---

## SNMP and NTP log rotate issues

### 1) SNMP log became too large / “error on subcontainer 'ia\_addr' insert (-1)” entries

- Refer to Mantis case 1871 and 2343.
- Per 1871 - SNMP log is apparently not rotated, but instead deleted upon boot-up??
- Per 2343

**Note:** This was observed a couple of different times, with a weird entry of “**error on subcontainer 'ia\_addr' insert (-1)**” being asserted and filling up the SNMP logs.

**Email from Paul Myers** about “subontainer entries” I found 3 possible reasons for this:

- 1) Snmpd.conf file which should be in /home/Spectracom/config/snmpd.conf was NOT present or found in any search path supported by snmpd.
- 2) Snmpd.conf is invalid and needs to be regenerated.

Httpd service loads processor and snmpd complains. (longshot)

Please see if /home/Spectracom/config has an snmpd.conf file.

Have them send that to you.

Can they reconfigure snmpd AFTER getting us the configuration file and stop/start SNMPD?

Also are they on a heavily loaded network?

Do they have multiple Ethernet ports?

Did they change IP addresses after setting up SNMPD?

Maybe we should have them setup networking THEN setup SNMP and shutdown/restart either the SecureSync OR shutdown and restart SNMP service.

Maybe it's a snmpd config file thing or an IP address issue with the daemon having trouble with ip addresses changing?

### 2) NTP log became too large (v4.8.9 and below)

- Refer to Mantis case 2182

**Note:** in versions 4.8.9 and below, this is likely due to too many “Buffer Overflow” entries being asserted in the NTP log (due to NTP v4.20 receiving a significant number of NTP request).

## FAQs regarding log rotations

Some info from the SecureSync'a manual regarding log rotation and deletion

### 4.12 Logs

SecureSync maintains different types of event logs (see below) to allow for traceability, and for record keeping. Should you ever require technical support from Spectracom, you may be asked for a copy of your logs to facilitate remote diagnosis.

Logs stored internally are being kept automatically, while the storage of log files in a remote location has to be set up by the user.

For each type of log, four 75 KB files are maintained internally on a revolving basis, i.e. the oldest file will be overwritten, as soon as all four files have filled up with event data. The life expectancy of a log file depends on the amount of data accumulating over time: Some types of logs will fill up within days, while others can take months until they have reached their maximum storage capacity.

Logs can be deleted by the user at any time, see "Clearing Logs" on page 272.

### Logs/entries associated with log rotation occurring

#### chron.log

fcron[4054]: Job /usr/sbin/logrotate /etc/logrotate.conf complete

## Other FAQs about log rotation/log rollovers

### Logrotate.conf configuration file

Q Configurable, or are we restricted to what is in /etc/logrotate.conf? /etc/logrotate.d appears to be locked down)

**A Keith's response (based on input from Paul M, 11 Apr 17) :** No, this configuration is restricted and fixed to ensure drive space preservation.

Q What is the limited size of the log files?

**A. Keith's response:** There is no set "size limit" to the log files. The log files are automatically checked every 10 minutes to see if they are at least 75kb in size. If they are, the log entries start to be rotated. If there are many log entries being made to any particular log file, they could be significantly larger than 75kb within the 10 minute interval between the log size checks. If they are any value about 75kb when checked, a new "log file" is created. Typically, the logs are between 75kb and 77kb, when they are checked at a 10 minute interval.

Q When the log files reach its limit, How is the new file created? I saw there are multiple files with .1, .2, .3,...etc, e.g. alarm.log, alarm.log.1, alarm.log.2, alarm.log.3. It seems that the file with the bigger number is the oldest file and the .1 file is the next most recent file and the .log file (with no number) is always the current file. Is that the way the SecureSync write log files?

**A Keith's response:** Yes! If a log is found to be over 75 kb when its checked at the scheduled 10 minute interval, the earlier log entries start to first rotate into a .1 log. Then, when the .1 log is found to be exceeding 75 kb, the oldest logs start to be rotated into the .2 log. This continues to occur until the .4 log is found to exceed 75 kb, at which time, the .4 file is deleted (leaving the log with no number – which has the most recent entries -as well as the .1, .2 .3 logs).

When viewing the logs in the web browser, all of the same log files (the ones with no number, as well as .1, .2, .3 and .4 –if they exist- will all be displayed together as one continuous log).

Q. On the GUI, after how many logs or after what time-period are the logs cleared?

**A. Reply from Keith** Each type of log (such as Event, Alarms, etc) are stored in separate "bundles". When a log is initially detected to be 75kb or larger, those log entries are rotated as a bundle with the name of the log incremented to 1. Then, when that type of log hits 75kb again, it rotates again, the name of the "original" logs that had rotated to "1" increments to "2". When the number is 4 and the logs rotate again, that particular bundle of logs is deleted.

The web browser displays all of the entries from all bundles of that log type that have not been deleted yet. So how many logs that can be retained and for how long they can be retained is completely dependent upon how many log entries of that log type are being asserted. The more log entries of particular log type that are being asserted, the sooner those bundles will reach "75kb" and the sooner they will be rotated out.

If it's desired to periodically archive logs to prevent them from being deleted/lost, there is a way for a user to generate a single file which contains all of the log bundles. Then, it can be pulled from the NTP server using FTP. Below is information about generating and exporting this log file.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session.

The log bundling is controlled in the "Tools"/ "Upgrade/Backup" page of the SecureSync's web browser. Click on the "Configuration" tab. Then, to bundle the logs, change "Save Log Files" to "Enabled" and then hit Submit. This generates a single file bundle of the logs. This file ("SecureSync.log") is placed in the "home/spectracom/xfer/log" directory. Once it has been created, you can FTP/SCP it off the box (just make sure "FTP Service" is enabled in the Network/General page of the browser, "Services" tab).

If you need a free FTP client, we often use CoreFTP (<http://www.coreftp.com/>).

Q Is there any configuration in the system which generates an alert if the memory reaches a configured threshold value?

**A** We periodically here this question, as well. Note this is written for your benefit and shouldn't be just copy/pasted to a customer- Because the logs do automatically rotate, there is little risk of the logs taking up too much space in the CF card, unless there happened to be a flood of logs asserted at the same time (since the logs are reviewed every 10 minutes to find out how large they are, a flood of log entries within the same 10 minute period, could potentially fill a log file before it had a chance to see if it needed to be rotated.

There is no automatic alert if the logs start to take up too much space on the CF card. However, a customer can always view how

much space on the CF card is currently being used by the system/free space still available, via the `df -h` CLI command, or via the "Disk Status" section on the **Tools** -> **Upgrade/Backup** page of the browser (starting in software version 5.2.1 as shown below):

| Disk Status |      |
|-------------|------|
| Total       | 947M |
| Used        | 467M |
| Free        | 431M |
| Percent     | 52%  |

Q Is there any mechanism which indicates us if the logs are deleted or overwritten?

A As log rotation and deletion is automatic, there is no "indication" for this operation occurring, other than either viewing the names of the files present in the `/home/spectracom/log` directory, or viewing the daemon log in this directory (which indicates logs were looked at to see if any logs needed to be rotated). As a number is added to the end of each log file in this directory once its rotated, having files with a number at the end "such as **alarms.log.1**" for instance) indicates that particular log file has been rotated. A log file that has a ".4" at the end of its name (such as "**alarms.log.4**") that particular set of log entries will be automatically deleted once that log files rotates again (the same file with numbers of .1, .2. and .3 will still be in the unit.

---

### Alerts associated with Log sizes

➤ Refer to Mantis case 2068

Q. Is there a setting in the system that will notify a remote logging server when the log file reaches a certain size (like 75%)?

A. As of at least version 5.3.0 there are no alerts associated with the size of the log files. The logs just rotate when they reach or exceed 75kb.

---

### Log Configuration/Mapping (Facility and Severity codes)

Logs are configured in the:

A) Newer web browser (versions 5.1.2 and above):

Management -> Log Configuration page, Center "Gear" ICON for each log type.

B) Classic interface browser: Setup -> Logs page of the browser

#### Email from Dave Sohn (3/16/12)

Facility and level are the syslog routing parameters to our log files. Our mapping is located in **config/speclog.conf**. By default the update log is local7.info

Below are the factory default log configurations.

**Note:** Changing either or both of the Facility and Priority codes will cause log entries to be mapped to the wrong log files.

Q How does one configure the logging level? The other logs are straightforward. This one is not.

A Keith's response: The **Management->Log Configuration** page of the web browser allows change of syslog facility/priority values, but as the combinations of these two values map log entries into their correct log files, please be aware that changing these codes can have the effect of mixing log entries with current log locations, making it much harder to analyze the internal logs (for example the hourly GNSS Qualification log entries could potentially end up being sent to the Alarms log (along with Alarms

logs entries), instead of being sent to the Qualification log where these entries are normally

**Note:** These have been updated since earlier software versions. The entries below are for at least versions 5.2.0, 5.2.1 and 5.30 -> 5.4.0.

| Log tab                  | Facility code | Priority code |
|--------------------------|---------------|---------------|
| System                   | Local Use 7   | Emergency     |
| Events                   | Local Use 7   | Alert         |
| Alarms                   | Local Use 7   | Critical      |
| Timing                   | Local Use 7   | Error         |
| GPS Qual (Qualification) | Local Use 7   | Warning       |
| Oscillator               | Local Use 7   | Debug         |
| Journal                  | Local Use 7   | Notice        |
| Update                   | Local Use 7   | Information   |
| Authentication           | N/A           | N/A           |

## Save Logs

### A) Save logs via web browser

#### 3. Using new (black/charcoal) browser (versions 5.1.2 and above)

All of the SecureSync's logs (including those shown in the browser and also those in the background) can be easily bundled into one file and then exported from the SecureSync to send as an attachment.

Instead of copy/pasting all of the log entries into a Word document, starting in Archive software update version 5.1.2, the logs can be easily saved to single bundled file and exported into a networked PC. Earlier versions of software allowed the bundle to be created, but then the file still needed to be transferred out using an FTP/SCP connection. Now, a button in the web browser alleviates the need to create an FTP session to transfer this file out to a PC.

The log bundling and export to a PC is controlled in the **"Management"** -> **"Log Configuration"** page of the SecureSync's web browser. On the left-side of the browser, click on the **"Save and download all logs"** button. You can then select where to save the log bundle to. The default file name is "securesync.log".

#### 4. Classic interface web browser

All of the SecureSync's logs (including those shown in the browser and also those in the background) can be easily bundled into one file and then exported from the SecureSync to send as an attachment.

In order to capture the log files, simply copy/paste all of the log entries (from all of the log tabs) in the SecureSync's **Tools** -> **Logs** page of its web browser (such as all of the log entries in the "Event" tab, "Alarms" tab, "Oscillator" tab, etc). Paste all of the log entries into a single Microsoft Word document and then send us this document for our review.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session. Then, simply attach this extracted file to a reply email. Below is additional information on how to bundle and extract all of the unit's logs:

The log bundling is controlled in the "Tools"/ "Upgrade/Backup" page of the SecureSync's web browser. Click on the "Configuration" tab. Then, to bundle the logs, change "Save Log Files" to "Enabled" and then hit Submit. This generates a single file bundle of the logs. This file ("securesync.log") is placed in the "home/spectracom/xfer/log/" directory. Once it has been created, you can FTP/SCP it off the box (just make sure "FTP Service" is enabled in the Network/General page of the browser, "Services" tab).

If you need a free FTP client, we often use CoreFTP (<http://www.coreftp.com/>).

## B) Save logs via CLI interface only (not using the web browser)

### 1. Versions 4.7.0 and above

- Logs can be placed into a single log file and then exported out using FTP/SCP:

CLI command to save the logs to a single file: **savelog** XXX<enter> (where xxx is the desired file name)

```
spadmin@Custservice177 ~/log $ savelog securesync_logs
/home/spectracom/xfer/log/securesync_logs
Creating Log Archive at /home/spectracom/xfer/log/securesync_logs
tar: Removing leading '/' from member names
tar: Removing leading '/' from hard link targets
tar: /home/spectracom/log/discstats: file changed as we read it
spadmin@Custservice177 ~/log $ █
```

Desire to manually FTP out the logs (not using the browser to bundle them first)

**Note:** All SecureSync Logs are stored in the **home/spectracom/log** directory.

1. Perform a **savelog xxx** <enter> command

```
spadmin@Custservice177 ~/log $ savelog securesync_logs
/home/spectracom/xfer/log/securesync_logs
Creating Log Archive at /home/spectracom/xfer/log/securesync_logs
tar: Removing leading '/' from member names
tar: Removing leading '/' from hard link targets
tar: /home/spectracom/log/discstats: file changed as we read it
spadmin@Custservice177 ~/log $ █
```

2. This file will be created and stored in the **home/spectracom/xfer/log** directory

```
spadmin@Custservice177 /home $ cd spectracom/xfer/log/
spadmin@Custservice177 ~/xfer/log $ ls
securesync.log securesync_logs
spadmin@Custservice177 ~/xfer/log $ █
```

3. Use an FTP program (such as CoreFTP lite freeware) or SCP out the files.

**Important Note:** Transfer out this file using **Binary** mode

---

### 2. Software versions prior to version 4.7.0

In software versions prior to version 4.7.0, go to **home/spectracom** directory and drag over the **log** directory to the computer to capture all of the logs

**Note:**

- FTP port is **port 21**
  - SCP port is **port 22**
- Starting in version 4.7.0, All Logs can be placed into a single log file and then exported out using FTP/SCP:

- Easier method to review logs: rename the file as .tar

Below is a good draft (both the blue and red below) to capture version, screenshots and logs for troubleshooting a GPS reception issue. The red by itself discusses just the log bundling.

I have a couple questions and requests for you, so that we can better help you get this issue resolved.

- What is the current Archive software version (as reported in the Tools -> Versions page of the browser).
- Attached for your reference is a document that discusses how to identify if a GPS reception issue is occurring with the SecureSync. If it is, it also discusses how to troubleshoot this condition.
- Please send me a screenshot capture of the Status -> Time and Frequency and Setup-> Reference Priority pages of the web browser.
- Please also send us all of the log entries from each of the tabs on the Tools-> Logs page of the browser, for our review. You can either copy/paste them to a Word document, or there is a method to bundle them into a single file and then with a FTP/SCP session, just export this file out of the box. Then email this file to us as an attachment.

**Below is information on how to bundle the logs:**

In order to capture the log files, simply copy/paste all of the log entries (from all of the log tabs) in the SecureSync's **Tools -> Logs** page of its web browser (such as all of the log entries in the "Event" tab, "Alarms" tab, "Oscillator" tab, etc). Paste all of the log entries into a single Microsoft Word document and then send us this document for our review.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session. Then, simply attach this extracted file to a reply email. Below is additional information on how to bundle and extract all of the unit's logs.

The log bundling is controlled in the "**Tools**"/ "**Upgrade/Backup**" page of the SecureSync's web browser. Click on the "Configuration" tab. Then, to bundle the logs, change "Save Log Files" to "Enabled" and then hit Submit. This generates a single file bundle of the logs. This file ("SecureSync.log") is placed in the "**home/spectracom/xfer/log**" directory. Once it has been created, you can FTP/SCP it off the box (just make sure "FTP Service" is enabled in the Network/General page of the browser, "Services" tab).

If you need a free FTP client, we often use CoreFTP Lite (<http://www.coreftp.com/>).

After sending us the logs, we will review them and let you know what we find. Please let me know if you have any questions on the reception troubleshooting document. Then, we can go from there!



---

## \*\*\*\*Deleting/Clearing log files

### A) Via the newer web browser (versions 5.1.2 and above)

**Note:** only clears the logs that are displayed in the browser (such as Qual, NTP, etc). This function does not clear the “system” logs in the background only (such as sys.log, daemon.log, kern.log, mail.log, rexd.log, cron.log, mysql\_create.log and system.log)

- All Spectracom logs can be cleared at the same time from the Management -> Log configuration page, “Clear All Logs” button (left side of the page).
- Individual logs can also be cleared from the Management -> Log configuration page. Click the “X” ICON to the right of the name of the log to be deleted. It will then prompt you if you wish to delete all of the entries in the particular log

### B) Via the Classic interface Web browser

- All “Spectracom” logs displayed in the browser can be cleared at the same time from the
- Setup -> Logs page, “General Settings” tab
- Individual logs can also be cleared from the Setup -> Logs page (in each log tab)

### C) Via the CLI interface (Telnet or SSH)

**Note:** Only clears the logs that are displayed in the browser (such as Qual, NTP, etc). This function does not clear the “system” logs in the background only (such as sys.log, daemon.log, kern.log, mail.log, rexd.log, cron.log, mysqls.log and system.log)

- Version 5.1.5 introduced the clearlogs CLI command
- Can't delete the logs via CLI before version 5.1.5
- As of at least versions 5.1.4 and below, the logs can only be deleted via the web browser or front panel “clean” command. Permissions prevent the ability to delete the logs by themselves without performing a clean command from the front panel or CLI interfaces.

### D) Via the clean command

All Logs (and configs) can be deleted via the front panel/CLI “**Clean**” command (there is currently no way from the front panel to delete just the logs). The keypad has a “**Cmd**” menu (in the main “**System**” menu). After selecting this “**Cmd**” menu, press the up or down buttons until “**Clean**” is displayed. Then press the green checkbox. Once cleaned, if the network settings are statically set, they will need to be reprogrammed and any other config changes that have been made will need to be reconfigured as desired.

## Identifying which SecureSync sent the raw log entries to the Syslog server

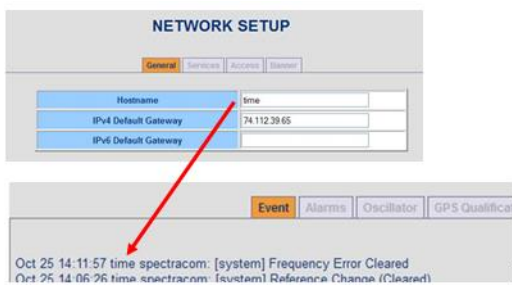
- Each log entries contain the DNS Hostname of the SecureSync.

**Note (Oct 31, 2012):** versions 4.8.7 and below were found to be sending a hard-coded “Spectracom” as the Hostname, even if the hostname is no longer this default value. So even if the hostname has been changed, the hostname will still be reported as “Spectracom”. This is supposed to be fixed in the next software release.

- (Danny Loke 10/26/12) However, they discovered that the raw logs do not contain any IP address. Thus, when the syslog are been logged to the remote syslog server, they are not able to determine which messages are been sent by which NTP servers.

**A (reply from Keith)** Syslog does not use IP addresses to identify the network device that sent the log entries. For DHCP networks, this would likely be very confusing, because IP addresses can and do change, as directed by the DHCP server.

So instead of sending the IP address with the log entries, syslog uses the DNS hostname to indicate the source of the raw log data. Each of the SecureSync (and NetClock) log entries includes the unit’s hostname. This is how to identify which SecureSync sent the logs. By factory default, the hostname for the time servers is “Spectracom”. Customers can change this value as they wish. For SecureSync, the hostname is configured in the **Network -> General Setup** page of the browser, **General** tab.



## \*\*NTPStats/NTP Statistics (loopstats, peerstats, clockstats and sysstats)

For technical info on these available NTP Logs, refer to the following in: [..\CustomerServiceAssistance.pdf](#)  
“NTP Statistics (NTP ClockStats, NTP loopstats and NTP Peerstats)”

- These NTP-specific logs are stored in the **/home/spectracom/log** folder
- These logs can be FTP/SCP transferred out or viewed using **telnet/ssh** as desired.
- Systats was added in version 5.2.1 (Not available in versions 5.2.0 and below)
- NTP’s loopstats, peerstats, clockstats(and sysstats starting in v5.2.1) are stored in the ntpstats folder in this directory (as shown in the screenshot below):

```
spadmin@Spectracom ~/log $ cd ntpstats
spadmin@Spectracom ~/log/ntpstats $ ls
clockstats          clockstats.28547C0  loopstats.20150324  peerstats.20150323
clockstats.20150327  input.plot          loopstats.20150325  peerstats.20150324
clockstats.20150328  loopstats           loopstats.20150331  peerstats.20150325
clockstats.20150329  loopstats.20150321 peerstats            peerstats.20150331
clockstats.20150330  loopstats.20150322 peerstats.20150321  peerstats.28547C1
clockstats.20150331  loopstats.20150323 peerstats.20150322
```

## Scheduled automatic FTP transfer of Stats/Extracting the NTP stats/NTP statistics files

- Automatic FTP transfer for NTP stats was added to NetClock 9300s as part of the Cachaca project for Brazil.



- This function was not carried over to SecureSyncs/NetClocks.

Refer to Salesforce Case 263627

**Email from Dave L to customer (6 May 2021)** This feature, formerly found in the Model 9300 series Netclocks, is not available in the new model Securesync or 9400 Series Netclocks.

To retrieve the NTP Statistics, NTP Statistics files can be manually FTP/SCP transferred out of the home/spectracom/log folder. NTP Stats CSV files can be manually transferred via the web browser or NTP Stats CSV files can also be automatically transferred (via a script) using the REST API interface.

The Web Ui will download the NTP Statistics csv files by selecting the Download button at the far right side of the Management/NTP Setup NTP Throughput section.

Using the REST API, the Securesync/Netclock REST API can be used to retrieve the NTP Statistics csv files from the Time Server. We have some information on the REST API: <https://www.rolia.com/documents/securesyncnetclock-9400-rest-api-collection-and-documentation>

1. NTP Statistics files can be manually **FTP/SCP transferred** out of the home/spectracom/log folder
2. NTP Stats CSV files can be manually transferred via the **web browser**
3. NTP Stats CSV files can also be automatically transferred (via a script) using the **REST API** interface

➤ Refer to case 207865 (excerpted below)

Q We are trying to pull NTP stats information so that we can monitor it from a remote server. Currently our process to get the NTP stats information is to painstakingly and individually download the logs bundle from each WebGUI management port but then we have to use 7zip to decompress it and then dig down and find the 'lafayette' file and then pull out the specific NTP Stats table from there. We have to do this on 30 servers so it is time consuming and not real time monitoring like we are looking to do. We have found the Lafayette file on the server, but due to it being owned by spfactory, we can't download it via the terminal. Is it possible to either:

A) Get access to the spfactory account

B) Can you provide us with a different method for consistently pulling the NTP stats data from all 30 of our current SpectraCom NTP devices to a remote server for monitoring?

We also found the ntp stats file via the terminal but it seems like that one only updates every hour and we are hoping to get more data than that.

A Per Dave L (6 Sept 2019) Yes, the Securesync/Netclock REST API can be used to retrieve the NTP Statistics csv files from the Time Server. We have some information on the REST API: <https://www.orialia.com/documents/securesyncnetclock-9400-rest-api-collection-and-documentation>

---

## Deleting the NTP Stats files (ntp statistics files)

### A) Ability to delete both the discstats and NTP stats (loopstats, peerstats, clockstats) via CLI

- Can't delete the NTPstats via CLI before version 5.1.5.
- Version 5.1.5 introduced the **clearstats** CLI command.

### B) Ability to delete the NTP stats (loopstats, peerstats, clockstats and sysstats) via newer web browser

Bottom-left corner of the **Tools** -> **Upgrade/Backup** page ("Clear All Stats" button).

## Software issue associated with deleting logs and NTP stats via the web browser

- With at least software versions 5.2.1 and below, these two browser buttons don't work.
- Note the associated CLI commands (clearlogs and clearstats) work fine in both Models (believe these were both added in version 5.1.5).
- Refer to Mantis case 3049.
- fixed in the version 5.3.0 update (Sept 2015)

## The various NTP Stats/NTP Statistics files

```
spadmin@Spectracom ~/log $ cd ntpstats
spadmin@Spectracom ~/log/ntpstats $ ls
clockstats      clockstats.28547C0  loopstats.20150324  peerstats.20150323
clockstats.20150327  input.plot          loopstats.20150325  peerstats.20150324
clockstats.20150328  loopstats           loopstats.20150331  peerstats.20150325
clockstats.20150329  loopstats.20150321  peerstats           peerstats.20150331
clockstats.20150330  loopstats.20150322  peerstats.20150321  peerstats.28547C1
clockstats.20150331  loopstats.20150323  peerstats.20150322
```

### A) Systats (versions 5.2.1 and higher) packet counts/status/version info

- From: <https://www.eecis.udel.edu/~mills/ntp/html/monopt.html>

**systats**  
Record system statistics. Each hour one line is appended to the `systats` file set in the following format:

```
50928 2132.543 3600 81965 0 9546 56 512 540 10 4 147 1
```

| Item     | Units | Description                |
|----------|-------|----------------------------|
| 50928    | MJD   | date                       |
| 2132.543 | s     | time past midnight         |
| 3600     | s     | time since reset           |
| 81965    | #     | packets received           |
| 0        | #     | packets for this host      |
| 9546     | #     | current versions           |
| 56       | #     | old version                |
| 512      | #     | access denied              |
| 540      | #     | bad length or format       |
| 10       | #     | bad authentication         |
| 4        | #     | declined                   |
| 147      | #     | rate exceeded              |
| 1        | #     | kiss-o'-death packets sent |

### B) Clockstats (Reference Clock drivers, such as System Time input to NTP)

- From: <https://www.eecis.udel.edu/~mills/ntp/html/monopt.html>

**clockstats**  
Record reference clock statistics. Each update received from a reference clock driver appends one line to the `clockstats` file set:

```
49213 525.624 127.127.4.1 93 226 00:08:29.606 D
```

| Item        | Units | Description             |
|-------------|-------|-------------------------|
| 49213       | MJD   | date                    |
| 525.624     | s     | time past midnight      |
| 127.127.4.1 | IP    | reference clock address |
| message     | text  | log message             |

The `message` field includes the last timecode received in decoded ASCII format, where meaningful. In some cases a good deal of additional information is displayed. See information specific to each reference clock for further details.

### C) *Loopstats* (NTP's internal clock)

- From: <https://www.eecis.udel.edu/~mills/ntp/html/monopt.html>

**loopstats**  
Record clock discipline loop statistics. Each system clock update appends one line to the `loopstats` file set:

50935 75440.031 0.000006019 13.778 0.000351733 0.013380 6

| Item        | Units              | Description                         |
|-------------|--------------------|-------------------------------------|
| 50935       | MJD                | date                                |
| 75440.031   | s                  | time past midnight                  |
| 0.000006019 | s                  | clock offset                        |
| 13.778      | PPM                | frequency offset                    |
| 0.000351733 | s                  | RMS jitter                          |
| 0.013380    | PPM                | RMS frequency jitter (aka wander)   |
| 6           | log <sub>2</sub> s | clock discipline loop time constant |

### D) *Peerstats* (other NTP servers listed in Peers/Servers tables)

- From: <https://www.eecis.udel.edu/~mills/ntp/html/monopt.html>

**peerstats**  
Record peer statistics. Each NTP packet or reference clock update received appends one line to the `peerstats` file set:

48773 10847.650 127.127.4.1 9714 -0.001605376 0.000000000 0.001424877 0.000958674

| Item         | Units | Description        |
|--------------|-------|--------------------|
| 48773        | MJD   | date               |
| 10847.650    | s     | time past midnight |
| 127.127.4.1  | IP    | source address     |
| 9714         | hex   | status word        |
| -0.001605376 | s     | clock offset       |
| 0.000000000  | s     | roundtrip delay    |
| 0.001424877  | s     | dispersion         |
| 0.000958674  | s     | RMS jitter         |

The status field is encoded in hex format as described in Appendix B of the NTP specification RFC 1305.

Peer status word (refer to: <https://www.eecis.udel.edu/~mills/ntp/html/decode.html#sys>)

File Edit View History Bookmarks Tools Help

Spectracom x SPECTRACOM CORP x Event Messages and Status... x

https://www.eecis.udel.edu/~mills/ntp/html/decode.html#sys

Summary Most Visited home page Software Updates Ap Notes ShareFile Case: 00002775 - sales... Switchboard - Extensio... Mailbox Startup servers Startup SAP Business ByDesign

### Peer Status Word

The peer status word consists of four fields: Status (0-4), Select (5-7), Count (8-11) and Code (12-15). It is reported in the first line of the `ev 00000000` display produced by the `stpq` program.

| Status | Select | Count | Code |
|--------|--------|-------|------|
|--------|--------|-------|------|

The Status Field displays the peer status code bits in hexadecimal; each bit is an independent flag. (Note this field is 5 bits wide, and combines with the the 3-bit-wide Select Field to create the first full byte of the peer status word.) The meaning of each bit in the Status Field is listed in the following table:

| Code | Message | Description            |
|------|---------|------------------------|
| 08   | bcac    | broadcast association  |
| 10   | rsach   | host reachable         |
| 20   | auth    | authentication ok      |
| 40   | authab  | authentication enabled |
| 80   | ccatig  | persistent association |

The Select Field displays the current selection status. (The T Field in the following table gives the corresponding tally codes used in the `stpq peer` display.) The values are coded as follows:

| Code | Message          | T | Description                                                       |
|------|------------------|---|-------------------------------------------------------------------|
| 0    | sel_nselect      | . | discarded as not valid (TEST10-TEST13)                            |
| 1    | sel_intersection | ^ | discarded by intersection algorithm                               |
| 2    | sel_overflow     | - | discarded by table overflow (not used)                            |
| 3    | sel_cluster      | - | discarded by the cluster algorithm                                |
| 4    | sel_combine      | * | included by the combine algorithm                                 |
| 5    | sel_backup       | # | backup (more than <code>tos</code> <code>maxclock</code> sources) |
| 6    | sel_sys_peer     | * | system peer                                                       |
| 7    | sel_pps_peer     | o | PPS peer (when the prefer peer is valid)                          |

The Count Field displays the number of events since the last time the code changed. Upon reaching 15, subsequent events with the same code are ignored.

The Event Field displays the most recent event message coded as follows:

| Code | Message          | Description                                  |
|------|------------------|----------------------------------------------|
| 01   | mobilitv         | association mobilized                        |
| 02   | demobilize       | association demobilized                      |
| 03   | unreachable      | server unreachable                           |
| 04   | reachable        | server reachable                             |
| 05   | restart          | association restart                          |
| 06   | no_reply         | no server found (stpsata mode)               |
| 07   | rate_exceeded    | rate exceeded (kiss code <code>rate</code> ) |
| 08   | access_denied    | access denied (kiss code <code>deny</code> ) |
| 09   | leap_armed       | leap armed from server LI code               |
| 0a   | sys_peer         | become system peer                           |
| 0b   | clock_event      | see clock status word                        |
| 0c   | bad_auth         | authentication failure                       |
| 0d   | popcorn          | popcorn spike suppressor                     |
| 0e   | interleave_mode  | entering interleave mode                     |
| 0f   | interleave_error | interleave error (recovered)                 |

### Clock Status Word

The clock status word consists of four fields: Unused (0-7), Count (8-11) and Code (12-15). It is reported in the first line of the `clock000 00000000` display produced by the `stpq` program.

| Unused | Count | Code |
|--------|-------|------|
|--------|-------|------|

The Count Field displays the number of events since the last `clock000` command, while the Event Field displays the most recent event message coded as follows:

| Code | Message    | Description |
|------|------------|-------------|
| 0a   | clk_errone | erroneous   |

status word ^ Highlight All Match Case 2 of 20 matches

File Edit View History Bookmarks Tools Help

Spectrac... rrr-ffff Main Me... Troub... x Case: 000... https://...nc.log Case: 000... Cases: H... > +

www.ntp.org/ntpfaq/NTP-s-trouble.htm#Q-TRB-MON-STATFIL

Search

Most Visited Yousendit Case: 00002775 ~ sales... https://10.2.100.58/cgi... Switchboard - Extensio... Google home page >>

### Table 3. Statistic Files

| File Type | Version | List of Fields                                                                        |
|-----------|---------|---------------------------------------------------------------------------------------|
| loopstats | 3       | day, second, offset, drift compensation, polling interval                             |
|           | 4       | day, second, offset, drift compensation, estimated error, stability, polling interval |
| peerstats | 3       | day, second, address, status, offset, delay, dispersion                               |
|           | 4       | day, second, address, status, offset, delay, dispersion, skew (variance)              |

```

50560 79386.259 127.127.8.1 9695 -0.001186 0.00000 0.00961
50560 79450.260 127.127.8.1 9695 -0.002161 0.00000 0.00528
50560 79514.261 127.127.8.1 9695 -0.003087 0.00000 0.00333

50560 79386.259 -0.001186 16.8701 6
50560 79450.260 -0.002161 16.8619 6
50560 79514.274 -0.003087 16.8501 6
50560 79578.295 -0.003959 16.8350 6

51801 71279.247 127.0.0.1 2194 0.000000609 0.000000000 0.000001023 0.000000000
51801 71279.248 127.127.22.1 9714 0.000001290 0.000000000 0.000000000 0.000000018
51801 71304.037 127.127.8.1 9434 0.000000879 0.000000000 0.000000000 0.000000032
51801 71339.248 127.127.22.1 9714 -0.000000076 0.000000000 0.000000000 0.000000028
51801 71368.038 127.127.8.1 9434 -0.000000129 0.000000000 0.000000000 0.000000046

51801 71143.245 0.000000594 17.526474 0.000000021 0.019386 6
51801 71279.248 0.000000609 17.556229 0.000000025 0.022492 6
51801 71404.250 -0.000000036 17.538976 0.000000023 0.021379 6

```

#### 8.1.3. How can I see the Time Difference between Client and Server?

(By [Terje Mathisen](#)) Normally `ntpd` maintains an estimate of the time offset. To inspect these offsets, you can use the following commands:

- `ntpq -p` will display the offsets for each reachable server in milliseconds (`ntpdc -p` uses seconds instead).
- `ntpdc -c loopinfo` will display the combined offset in seconds, as seen at the last poll. If supported, `ntpdc -c kerninfo` will display the current remaining correction, just as `ntptime` does.

The first can be used to check what `ntpd` thinks the offset and jitter is currently, relative to the preferred/current server, the second can tell you something about the estimated offset/error all the way to the stratum 1 source. [Q: 8.1.2](#) describes a way to collect such data automatically.

Loopstats/peerstats from <http://www.ntp.org/ntpfaq/NTP-s-trouble.htm#Q-TRB-MON-STATFIL>

Table 3. Statistic Files

| File Type | Version | List of Fields                                                                        |
|-----------|---------|---------------------------------------------------------------------------------------|
| loopstats | 3       | day, second, offset, drift compensation, polling interval                             |
|           | 4       | day, second, offset, drift compensation, estimated error, stability, polling interval |
| peerstats | 3       | day, second, address, status, offset, delay, dispersion                               |
|           | 4       | day, second, address, status, offset, delay, dispersion, skew (variance)              |



---

### **\*\*“Awk” and “Sed” filters for logs**

- Refer to <http://en.wikipedia.org/wiki/Sed>
- We don't have any log filters

Q. Do you have some handy “awk” or “sed” filters appropriate for log file analysis? Or any other tools?

**A. Reply from Dave Sohn (21 Jan 2014)** I don't have any filters in general for the logs.

**A. Reply from Paul Myers (21 Jan 2014)** We make them as we need them.

---

**\*\*Specific log file entries**

| Log                                                    | Refer to Section below                            |
|--------------------------------------------------------|---------------------------------------------------|
| Alarms.log                                             | <a href="#">Alarms log</a>                        |
| Auth.log<br>(Authentication)                           | <a href="#">Auth log (Authentication log)</a>     |
| Cron.log (Cron)                                        | <a href="#">cron.log (Cron log entries)</a>       |
| Daemon.log                                             | <a href="#">daemon.log</a>                        |
| Discstats                                              | <a href="#">Discstats</a>                         |
| Error.log<br>("ssl_request_log"<br>(apache access log) | <a href="#">Error log</a>                         |
| Events.log                                             | <a href="#">Events log</a>                        |
| Qual.log<br>(Qualification)                            | <a href="#">Qual log</a>                          |
| Journal.log                                            | <a href="#">Journal log</a>                       |
| Kern.log (Kernel<br>log)                               | <a href="#">Kernel Log</a>                        |
| Mail.log                                               | <a href="#">Mail.log</a>                          |
| Manifest.log                                           | <a href="#">manifest.log/manifest.config file</a> |
| Mysql_create.log                                       | <a href="#">Mysql_create.log</a>                  |
| NTP.log                                                | <a href="#">NTP log</a>                           |
| Oscillator.log<br>(osc.log)                            | <a href="#">Oscillator log</a>                    |
| Raccoon.log                                            | <a href="#">rc.log (raccoon)</a>                  |
| Rexd.bone                                              | <a href="#">_rex.d.bone</a>                       |
| rex.d.log                                              | <a href="#">rex.d.log</a>                         |
| Qual.log                                               | <a href="#">qual.log</a>                          |
| SNMPd.log                                              | <a href="#">SNMPd.log</a>                         |
| Rc.log (raccoon)                                       | <a href="#">rc.log (raccoon)</a>                  |
| Sys.log (syslog)                                       | <a href="#">sys.log</a>                           |
| System.log                                             | <a href="#">System log</a>                        |
| Timekeeper.log                                         | <a href="#">Timekeeper.log</a>                    |
| Timing.log                                             | <a href="#">Timing log</a>                        |
| Transfer.log                                           | <a href="#">Transfer.log</a>                      |
| Update.log                                             | <a href="#">Update log</a>                        |
| User.log                                               | <a href="#">User log</a>                          |
| Wtmp.log                                               | <a href="#">wtmp.log file</a>                     |

## Alarms.log (Alarms log)

### In Holdover:

- Caused by loss of all input references.

**Note: Time server is still in sync while in Holdover mode.**

---

### Not in Sync:

#### Caused by:

- Holdover mode expiring with no references being restored.
- Reboot/power cycle, until; resyncs to a reference.

---

### Host disciplining (NTP disciplining the TCXO/OCXO oscillator) (applicable to versions 5.3.0 and above)

[system] 2015 289 16:31:24 001 HR: Enabling Host Disciplining Mode

- **This entry is asserted each time KHTD is restarted (as indicated in the System log):** KTS Host Time Daemon has restarted (KHTD)

---

Frequency error alarm- Indicates the internal reference oscillator has experienced a large frequency correction.

**The Frequency Error Alarm is asserted when 10 MHz Frequency Error measurement exceeds a set threshold (oscillator dependent)**

- **TCXO oscillator:**  $1 \times 10^{-7}$  in v5.3.0 and below (changed to  $1 \times 10^{-6}$  starting in v5.3.1 to address. See note below about Mantis case 3168)
  - **OCXO oscillator”**  $1 \times 10^{-8}$
  - **Rubidium (and low phase noise Rubidium-LPN Rb):**  $1 \times 10^{-9}$
- Frequency Error Alarm clears once the measured frequency error no longer exceeds the applicable threshold.
  - Frequency Error Alarm is only ever asserted if a disciplining reference (such as GPS) is present/valid (it's not asserted when there is no reference available).

### This alarm occurs when:

- Power-up (clears shortly after TFOM gets down to TFOM 3 or below - phase error less than 100ns)
- loss of all input references
- Synced to NTP or Self
- 10 MHz Frequency Error measurement exceeds  $1 \times 10^{-8}$

---

**Timing System Software Error:** This entry can indicate an issue with the 10 MHz oscillator or GPS receiver (such as the oscillator being affected by the RES-SMT-GG GPS receiver, with v1.06 firmware)

- Have observed it as a factor of initial boot-up
- Have observed it with a Compact Flash (CF) card needing to be replaced

**Note: In earlier software versions (such as v5.1.4 or 5.1.5 for examples), this alarm can potentially be asserted in the logs as a “minor, spurious reporting-issue only”**

**email from Dave L (26 Jun 18)** Also, I found some information on the “Timing System Software Error” message. I confirmed that the specific Timing System Error entry you observed being asserted in the logs is a minor, spurious reporting-issue only. There is a condition that can potentially cause this entry to be asserted with older software versions such as v5.1.5

installed. This entry is limited to just a logging condition and does not indicate the operation of the time server was affected. This minor logging issue was resolved with a subsequent software update.

Have seen it correlated with both of the following two log entries also being asserted at the same time:

- “Error:CS\_Set(CS\_SA\_LEAP\_SEC) call from GR” (in the Timing log)
- “Rb Reference unstable” (in the Oscillator log)
- Can be caused by the following error condition being asserted: CS\_Set(CS\_SA\_LEAP\_SEC) call from GR”. This failure is caused by software issues with the Res-SMT-GG receiver (v1.06 firmware) .
- Have also seen it asserted in conjunction with Holdover/Frequency Error alarms and Reference unstable” (in the Oscillator log). Examples below:

#### Example entries

```
Sep 16 05:04:35 No Longer In Holdover
Sep 16 05:04:35 Timing System Software Error
Sep 16 05:04:36 Reference Change (Cleared)
Sep 16 05:04:36 Timing System Software Error (Cleared)
```

```
Oct 17 06:48:39 Timing System Software Error
Oct 17 06:48:40 Timing System Software Error (Cleared)
```

---

**Timing System Hardware error:** This entry can indicate an issue with the 10 MHz oscillator or FPGA.

- Seen it asserted in conjunction with Holdover/Frequency Error alarms.

#### Diagnosing the Timing System Hardware Error entry:

1. Review the **Timing** log for entries that indicate a problem with the Rb osc, such as the following examples:

```
Rb fault detected
Oscillator module requires maintenance
Rb varactor error
Rb peak voltage error
Oscillator module resumed normal operation (only asserted, if the RB oscillator alarms are being asserted and clearing, as
an intermittent condition. It may not be asserted, with the others in this list)
```

```
[system] 2014 232 19:46:01 000 Rb varactor error (val=0, min=102, max=153)
[system] 2014 232 19:46:01 000 Rb peak voltage error (val=0, min=51, max=255)
[system] 2014 232 19:46:01 000 Rb fault detected (state=9)
```

2. Review the **Oscillator** logs for entries that indicate a potentially bad Rb oscillator, such as the following examples:

```
[system] 2014 204 12:49:19 000 XOS: Rb synchronized
[system] 2014 204 12:48:47 000 XOS: Rb tracking
[system] 2014 204 12:44:34 000 XOS: Rb track off -- free run
```

**Note:** Review the GPS Qual log to verify if “Rb track off -- free run” entries are due to a reception issue.

**Review the Alarms log to see if there are any “1PPS Not in specification” entries**

---

**“GPS Antenna Problem”**: Open or short has been detected in the antenna cable.

**“1PPS not in Specification” / “1PPS Restored to Specification” log entries**

**Note:** these entries will likely be coupled with Holdover alarms (and Qual logs that may look great)

These are events that occur and alarm entries that are asserted. “1PPS not in Specification” occurs if the current TFOM values exceed the user-configurable max TFOM value. When the TFOM falls below Max TFOM, the Restored to Specification event/alarm entry is asserted.

Regarding the “1PPS Not in Specification” alarm, this alarm only occurs if the current TFOM exceeds the user-configurable max TFOM value. The SecureSync going into Holdover mode will not initially and automatically cause the TFOM to increase and exceed the max TFOM value. However, if the unit continues to operate for an extended period of time without any valid input references, the oscillator will begin to drift. As long as the max TFOM is not set to 15, eventually, the max TFOM will be exceeded and the alarm is asserted. The type of oscillator (OCXO or Rubidium) and the setting of max TFOM will determine the typical amount of time in holdover required to exceed the max TFOM.

These alarms can even be asserted with great GPS Reception in Qual logs

**A) Classic interface browser**

**Email sent to a customer that had these alarms**

With a quick reminder from our Engineering team, I believe I now finally understand what is very likely causing the alarms to be asserted, even with great GPS reception!

This is an easy check to make. And if it's what we believe it is, is also just as easy to fix, as well!

Please navigate to the **Setup -> Disciplining** page of the browser. As shown below, what is the **“Maximum TFOM for Sync”** field set to (in version 4.8.6, I believe this was abbreviated as **“Max TFOM”**)?



TFOM **15** is the factory default value which will allow any TFOM value be acceptable for sync. We suspect that you may currently have a much lower MaxTFOM value configured, such as a “3” for instance. MaxTFOM of a lower value will cause the SecureSync to go into Holdover mode, if the SecureSync’s TFOM value exceeds this set value. It will remain in Holdover mode until the TFOM value no longer exceeds this set value. If TFOM is exceeded, GPS is considered “not valid” as a reference, resulting in the SecureSync being in Holdover mode and the alarm entries you are observing being asserted!!

The simple fix I to this is to increase the TFOM to a higher value that wouldn’t occur with good GPS reception. If you wish for SecureSync to go into Holdover based on the estimated accuracy value (RTFOM), set it to a value such as a 5 or a 6, for instance. If you prefer it not to go into Holdover mode based on the TFOM value, just change it back to 15.

Please let me know if it was set to a very low number, such as a 2 or 3 for instance!

---

## Auth.log (Authentication log)

- Generated from PAM (Pluggable Authentication Module) - not from apache  
<https://www.netbsd.org/docs/guide/en/chap-pam.html>
- Located in /home/spectracom/log auth.log

**/home/spectracom/log auth.log** – Contains system authorization information, including user logins and authentication mechanisms that were used.

### Authorization Log (from <https://help.ubuntu.com/community/LinuxLogFiles>)

The Authorization Log tracks usage of authorization systems, the mechanisms for authorizing users which prompt for user passwords, such as the Pluggable Authentication Module (PAM) system, the sudo command, remote logins to sshd and so on. The Authorization Log file may be accessed at /var/log/auth.log. This log is useful for learning about user logins and usage of the sudo command.

Use grep to cut down on the volume. For example, to see only information in the Authorization Log pertaining to sshd logins, use this: `grep sshd /var/log/auth.log | less`

Auth log / Ability to send Auth log entries to Syslog

- Versions 5.0.0 and below don't have a tab to view the Auth log in the web browser (it can be viewed via telnet, ssh or FTP)
- Version 5.0.1 adds an Auth log tab to the **Tools** -> **Versions** page of the Classic interface.
- As of at least version 5.01, the Auth log cannot be configured to be sent to a syslog server. (Update - Version 5.1.2, January 2014, adds the ability for this log to now be able to go to Syslog)

---

## Successful logins (browser and CLI interfaces)

Q Can the Authorization log be set to record successful logins and logouts?

A The Auth (Authorization) log is a log generated and maintained exclusively by the PAM module (Pluggable Access Module) PAM is the software module we use for login (The Auth log is not a "Spectracom" log). The Auth log has entries asserted for failed web browser and CLI (telnet, ssh, etc) logins. It also has entries asserted for successful CLI Logins. However, the PAM module does not assert any log entries for successful web browser login.

If a successful login occurs and the user makes any changes while logged in, these changes (including the user account name, date and time) is recorded in the Journal log (displayed in the **Tools** -> **Journal** page of the browser).

---

## Notes (as included in Auth log messages):

### Word after host name (such as "Spectracom")

- **sshd**- entry is associated with SSH login
- **fcron**- entry is associated with cron scheduler (such as log rotate)
- **xinetd** Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are relocated in the /etc/xinetd.d directory.
- **(pam\_unix)** This is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the /etc/passwd and the /etc/shadow file as well, if shadow is enabled.
- **(pam\_ldap)** The pam\_ldap module is a Pluggable Authentication Module (PAM) which provides for authentication, authorization and password changing against LDAP servers
- **(pam\_tally)** This module maintains a count of attempted accesses, can reset count on success, can deny access if too many attempts fail.

Note “/dev/tty” is referring to the **CLI interface**

### Password Change Attempt Logging

a) Is this treated differently between execution by a privileged (admin) user against another account vs. given account?

**Keith's response:** NO. It's not treated differently.

b) Is it logged at all (success and/or failure)?

**Keith's response:** Successful change is logged, Errors are not logged.

---

## Entries associated with tcpdump

**A) No auth log entries are asserted when starting tcpdump normally.**

**B) Trying to start tcpdump using “su” instead of “sudo” (or just typing “tcpdump” by itself)**

Note-omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE

- Note the correct command to start tcpdump is either “**tcpdump**” (v5.4.5 and above), or “**sudo tcpdump**” (v5.4.1 and below)

```
su[8096]: pam_unix(su:auth): authentication failure; logname=spadmin uid=1002 euid=0 tty=/dev/pts/2 ruser=spadmin rhost=
user=tcpdump
```

```
su[8096]: FAILED su for tcpdump by spadmin
```

```
su[8096]: - /dev/pts/2 spadmin:tcpdump
```

---

## Successful/unsuccessful login entries in the auth.log file

**A) HTTP/HTTPS (web browser login)**

- **Successful HTTP/HTTPS authentication:** No log entry sent from radius server
- **Unsuccessful HTTP/HTTPS authentication:** Log entry sent from radius servers and then local login is attempted.

**B) HTTP/HTTPS (web browser login using LDAP and Radius login)**

- **Successful LDAP/Radius authentication:** No log entry sent from a LDAP/Radius and no log entry in auth.log.
- **Unsuccessful LDAP/Radius authentication:** Log entry sent from radius servers LDAP/Radius and log entry asserted in auth.log.

**C) CLI interface (telnet/ssh/ftp login)**

- **Successful CLI interface authentication:** Log entry asserted in auth.log
- **Unsuccessful CLI interface authentication:** Log entry asserted in auth.log.

Q I am unable to find any log in/log out logs for audit. There seems to be only fail login present.

**A Keith's response:** This is a correct understanding for the web browser login. However, there are log entries for successful CLI logins (such as SSH connections).

The Auth (Authorization) log is a log generated and maintained exclusively by the PAM module (Pluggable Access Module) PAM is the software module we use for login (The Auth log is not a “Spectracom” log). The Auth log has entries asserted for failed web browser and CLI (telnet, ssh, etc) logins. It also has entries asserted for successful CLI Logins. However, the PAM module does not assert any log entries for successful web browser login.

If a successful login occurs and the user makes any changes while logged in, these changes (including the user account name, date and time is recorded in the Journal log (displayed in the **Tools** -> **Journal** page of the browser).

Below is an example Auth log entry indicating a **successful** ssh login:

SSH: Server;Ltype: Kex;Remote: 10.2.100.124-49468;Enc: aes256-ctr;MAC: hmac-sha2-256;Comp: none

---

## \*\*Authentication Log File Format

The first five fields in every authentication log entry are required by Steel-Belted Radius Carrier:

- Date—The date when the event occurred
- Time—The time when the event occurred
- RAS-Client—The name or IP address of the RADIUS client sending the authentication request
- Full-Name—The fully distinguished name of the user, based on the authentication performed by the RADIUS server
- ACC/REJ—The result of the authentication request (ACCEPT or REJECT)

The following example shows the heading line and an authentication log file entry consisting of the required attributes.

"Date","Time","RAS-Client","Full-Name","ACC/REJ"  
"7/3/2003","12:11:55","RRAS","EdisonCarter","ACCEPT",

“(from `getpwnam()` This is an entry at the very end of an auth log message

<http://pubs.opengroup.org/onlinepubs/009604599/functions/getpwnam.html>

**The `getpwnam()`** function shall search the user database for an entry with a matching *name*.

Example from a customer log:

Oct 21 21:33:10 ntp1-clf-6 httpd(pam\_unix)[17266]: could not identify user (from `getpwnam(smuthu)`) –  
(Where “**smuthu**” in parenthesis is the username that was entered)

Errors

[EIO]

An I/O error has occurred.

[EINTR]

A signal was caught during `getpwnam()`.

[EMFILE]

{OPEN\_MAX} file descriptors are currently open in the calling process.

[ENFILE]

The maximum allowable number of files is currently open in the system.

The `getpwnam_r()` function may fail if:

[ERANGE]

[TSF](#)  Insufficient storage was supplied via *buffer* and *bufsize* to contain the data to be referenced by the resulting **passwd** structure.

---

## Example Auth log entries

### ttyS0: input overrun

**Email from Dave Lorah to Verizon-** The Authorization Log entry `ttyS0: input overrun` message indicates there is a buffer overflow condition. This could be caused by short bursts of traffic that overrun the input. I will check with engineering to see if there is anything more I can tell you.

---

“**Conversation failed**” and “**tally undeflowed for user spadmin**” entries)

- Refer to salesforce case 24514



➤ Refer also to wtmp file: [wtmp.log](#)

This particular customer had three units (mix of versions of 5.4.1 and 5.4.5) with these two entries present. He reported trouble logging into the browser due to being “locked out of the spadmin account”. His report below”

Recently I noticed some of SecureSync in MRT couldn't be accessed through Web UI. I was able to open login page but when I enter user and password it stated wrongly user and password. I have login through telnet and below is the appeared message: Account locked due to 39347 failed logins, Account locked due to 32010 failed logins, and Account locked due to 2362 failed logins.

So I have reboot the unit and now can access the Web UI. Please advise is due from what?

*Sample of the Auth log entries below:*

```
2:31 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): conversation failed
Feb 21 07:52:31 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): user spadmin (1002) tally 39348, deny
5
Feb 21 07:52:34 SURS-CLK-SUBMC-00008 apache2: pam_unix(httpd:auth): authentication failure; logname=
uid=1001 euid=1001 tty= ruser= rhost=10.12.21.49 user=spadmin
Feb 21 07:52:34 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): conversation failed
Feb 21 07:52:34 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): user spadmin (1002) tally 39349, deny
5
Feb 21 07:52:44 SURS-CLK-SUBMC-00008 login[1828]: pam_unix(login:auth): authentication failure; logname=
uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=10.12.122.4 user=spadmin
Feb 21 07:52:45 SURS-CLK-SUBMC-00008 apache2: pam_unix(httpd:auth): authentication failure; logname=
uid=1001 euid=1001 tty= ruser= rhost=10.12.11.49 user=spadmin
Feb 21 07:52:46 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): conversation failed
Feb 21 07:52:46 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): user spadmin (1002) tally 39350, deny
5
Feb 21 07:52:47 SURS-CLK-SUBMC-00008 login[1828]: FAILED LOGIN (1) on '/dev/pts/1' from '10.12.122.4' FOR
'spadmin', Authentication failure
Feb 21 07:52:58 SURS-CLK-SUBMC-00008 login[1828]: pam_unix(login:session): session opened for user mrt1 by
(uid=0)
Feb 21 10:56:36 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 11:14:05 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 11:18:15 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 11:25:45 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 12:11:33 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
```

**Results of this case:** We suspect the wtmp file (records the logins and logouts was completely full due to potential authenticated security scans, Refer to [wtmp.log](#) in this doc for more info.

---

### fcron associated Auth log example entries

Spectracom fcron(pam\_unix)[16819]: account root has password changed in future:

The System Time has been set back in time/date (likely due to a user manually setting the time/date back to a previous date). This log entry will continue to be asserted, until the System Time has been brought back to the expected date/time.

**Status update:** this issue was reportedly fixed in the version 5.0.0 software update. Refer to Mantis case 2091 (<http://cvsmantis.int.rolia.com/mantis/view.php?id=2091>)

---

## HTTPS/web browser login associated auth log example entries

### Successful “spadmin” account login (not user accounts – user account login further below)

Username of “spadmin” /correct password (valid login)

Oct 23 15:33:13 Spectracom pam\_tally[7490]: pam\_tally: unknown option; reset

---

### Failed “root” account login, using an arbitrary password

#### Username of “root” / arbitrary password

16:18:58 Spectracom apache2: pam\_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser= rhost= user=root

16:18:58 Spectracom unix\_chkpwd[30840]: password check failed for user (root)

---

### Unsuccessful login using valid username but invalid password

Username of “spadmin” /wrong password (invalid login)

Spectracom httpd(pam\_unix)[11894]: authentication failure; logname= uid=1111 euid=1111 tty= ruser= rhost= user=spadmin

**Cause:** this one entry generated when I tried logging in with web browser, using the correct “spadmin” account name but the wrong password.

---

### Unsuccessful login using invalid username and arbitrary password

#### Invalid username of “admin1111” /erroneous password (invalid login)

14:22:34 Spectracom pam\_tally[11581]: pam\_tally: pam\_get\_uid; no such user

14:22:34 Spectracom httpd(pam\_unix)[11581]: authentication failure; logname= uid=1111 euid=1111 tty= ruser= rhost=

14:22:34 Spectracom httpd(pam\_unix)[11581]: check pass; user unknown

**Cause:** these three entries were generated when I tried logging in with web browser, using the incorrect “spadmin” account name of “admin1111” and just an arbitrary password.

---

### Hitting the logout button while logged in as spadmin

**Result:** No Auth log entries asserted

---

### Custom user account login

Just after creating new user account name of ‘kwing”

Oct 23 15:42:03 Spectracom pam\_tally[32593]: pam\_tally: unknown option; reset

Oct 23 15:41:20 Spectracom passwd(pam\_unix)[31574]: password changed for kwing

Oct 23 15:41:20 Spectracom chage[31570]: changed password expiry for kwing

Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to shadow group `spuser'

Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to shadow group `spadmin'

Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to group `spuser'

Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to group `spadmin'

Oct 23 15:41:19 Spectracom useradd[31569]: new user: name=kwing, UID=1113, GID=111, home=/home/spectracom, shell=/bin/bash

### **Username of “kwing” /correct password (valid login)**

Spectracom pam\_tally[9494]: pam\_tally: unknown option; reset (same as logging in as spadmin)

### **Username of “kwing” /wrong password (invalid login)**

Spectracom httpd(pam\_unix)[13910]: authentication failure; logname= uid=1111 euid=1111 tty= ruser= rhost= user=kwing

**Cause:** Account “kwing” does exist, but password not correct.

### **Invalid username “admin1111” /erroneous password (invalid login)**

Oct 23 15:49:57 Spectracom pam\_tally[16126]: pam\_tally: pam\_get\_uid; no such user

**Cause:** there is no user account with this name.

---

## **SSH login associated example entries**

Spectracom sshd[19393]: SSH: Server;Ltype: Authname;Remote: 10.253.96.80-32089;Name: ikkhan [preauth]

Spectracom sshd[19393]: Invalid user ikkhan from 10.253.96.80

Spectracom sshd[19393]: input\_userauth\_request: invalid user ikkhan [preauth]

Spectracom sshd[4195]: Accepted password for gvantrie from 10.21.32.66 port 1589 ssh2

Spectracom sshd[4195]: pam\_unix(sshd:session): session opened for user gvantrie by (uid=0)

Spectracom sshd[16833]: User root from 10.252.152.134 not allowed because none of user's groups are listed in AllowGroups

Spectracom sshd[16833]: input\_userauth\_request: invalid user root [preauth]

Spectracom sshd[16833]: Connection closed by 10.252.152.134 [preauth]

Spectracom xinetd[824]: EXIT: ssh pid=16833 duration=1(sec)

### **Custom username of “kwing” / correct password (valid login)**

Spectracom sshd[32499]: error: open /dev/tty failed - could not set controlling tty: Permission denied

Spectracom sshd(pam\_unix)[32278]: session opened for user kwing by (uid=0)

---

### **Username of “spadmin” /wrong password (invalid login)**

Spectracom sshd[12306]: error: PAM: Authentication failure for spadmin from pm-wing2.int.oroia.com

Spectracom sshd(pam\_unix)[12512]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=pm-wing2.int.oroia.com user=spadmin

**Cause-** Both entries generated when I tried logging in with SSH, using the correct “spadmin” account name but the wrong password

---

### **Invalid username “/correct spadmin password (invalid login)**

Spectracom sshd[27122]: Postponed keyboard-interactive for invalid user admin from 10.2.100.29 port 1280 ssh2 [preauth]

Spectracom sshd[27122]: Failed keyboard-interactive/pam for invalid user admin from 10.2.100.29 port 1280 ssh2

Spectracom sshd[27122]: error: PAM: User not known to the underlying authentication module for illegal user admin from pm-wing2.int.oroia.com

**Cause:** All three entries generated when I tried logging in with SSH, using the incorrect “spadmin” account name of “admin” , and the correct password of “admin123:

---

### **Exited out of a valid Putty session (just closed putty)**

Spectracom xinetd[782]: EXIT: ssh pid=26141 duration=156(sec)  
Spectracom sshd(pam\_unix)[26141]: session closed for user kwing

---

### **Clockstats (ntpstats)**

- The NTP clockstats are located in the ntpstats folder
- Search the log bundle for “clockstats” / “127.127.45.0” OR rename the entries in the log folder as .xls to view the data.
- 127.127.45.0 (Spectracom Reference Clock Driver) Entries indicate each time that NTP got a time input to System Time.
- Should be 16 seconds between each entry (based on the poll interval of our reference clock driver)
- Refer to clockstats in the NTP for all products section of this document for more info.

## discstats

- These oscillator-specific logs are stored in /home/spectracom/log directory
- These logs can be FTP/SCP transferred out or viewed using telnet/ssh, as desired
- Discstats are stored in the discstats folder in this directory (as shown in the screenshot below).
- Discstats are also included in the log bundle.

```
admin@Spectracom ~/log $ cd discstats
admin@Spectracom ~/log/discstats $ ls
discstats.20150327  discstats.20150329  discstats.20150331
discstats.20150328  discstats.20150330  input.plot
```

- Selected Time/PPS reference, DAC value, Phase Error, Frequency Error, internal Temperature (starting in version 5.2.0, if a temperature sensor is installed)
- Records 5 days of data for the oscillator disciplining plots (Management -> Disciplining page of new browser)
- 5 daily Logs are located in the discstats folder of the log bundle
- Search the log bundle for “discstats” or rename the 5 entries in the log folder as .xls (or even better, .csv to separate the columns as described below) to view the data

**Recommendation to better review these files:** Rename the files with the extension of “.CSV” . The files will still open with Excel, but the comma delimited values will be in separate columns, instead of all values being in the same column when just opening as a standard excel file.

### Data reported

- Data reported includes (left to right) Days since 1 Jan 1970, UTC Time Of Day (Seconds since midnight), Sync and Holdover status, selected Time/PPS reference , DAC value, Phase and Frequency Errors and Temperature (in versions 5.2.0 and above if a temp sensor is installed)

#### A) Software versions 5.2.0 and above (added internal temperature if thermostat is installed)

| Days   | TOD(S) | Sync | Holdover | REF         | DAC    | Phase Error(ns) | Freq Error | Temp (c)  |
|--------|--------|------|----------|-------------|--------|-----------------|------------|-----------|
| 16591, | 205,   | 1,   | 0        | ,ird0,ird0, | 33384, | 16,             | 8.94e-14   | 58.996452 |

#### B) Software versions prior to version 5.2.0

| Days  | TOD(S) | Sync | Holdover | REF        | DAC | Phase Error(ns) | Freq Error |
|-------|--------|------|----------|------------|-----|-----------------|------------|
| 16203 | 2789   | 1,   | 0        | gps0,gps0, | -3  | 33164           | -4.77e-11  |

**Days** = Number of Days since UNIX Epoch (1 Jan 1970)

**Available converter** (enter start date of **01/01/1970**)

- <http://www.timeanddate.com/date/durationresult.html?m1=01&d1=01&y1=1970&m2=05&d2=13&y2=2014>
- 

**TOD(S)** = Number of seconds since midnight on that day

**Total Range** is 0 to 86400

**Partial hours (add this value to the previous whole hour value)**

- **Seconds to xx:15**=900
- **Seconds to xx:30**=1800
- **Seconds to xx:45**=2700

| Time Seconds  | Time Seconds  |
|---------------|---------------|
| 00:00 = 0000  | 12:00 = 43200 |
| 01:00 = 3600  | 13:00 = 46800 |
| 02:00 = 7200  | 14:00 = 50400 |
| 03:00 = 10800 | 15:00 = 54000 |
| 04:00 = 14400 | 16:00 = 57600 |
| 05:00 = 18000 | 17:00 = 61200 |
| 06:00 = 21600 | 18:00 = 64800 |
| 07:00 = 25200 | 19:00 = 68400 |
| 08:00 = 28800 | 20:00 = 72000 |
| 09:00 = 32400 | 21:00 = 75600 |
| 10:00 = 36000 | 22:00 = 79200 |
| 11:00 = 39600 | 23:00 = 82800 |

- **Sync and Holdover:** “1” is true, “0” is False
- **DAC:** Believe this is the scaled DAC value for graph (not the actual DAC value)???
- DAC value range for TCXOs and OCXOs is 00000 to max 65535
  - **Min D/A:** 0x0000 (00000 in decimal)
  - **Max D/A:** 0xFFFF (65535 in decimal)
- **Phase error:** (in nanoseconds) Refer to the TFOM table to determine TFOM based on phase error

### Reported Frequency Error values

- Reported Frequency Error measurements are “raw” frequency error – not fractional frequency errors.
- These “raw” frequency error values are like 0.00076, 1 x 10 +/- 4, or 1 x 10 +/- 5, (not like the fractional frequency error values such x10<sup>-11</sup>, or x10<sup>-12</sup> like we are used to seeing in the Osc log)

### Freq error of 0.00e+00

**Per Dave Sohn (15 May 2014)** Seeing a zero value for the frequency error is not an indicator of any issues. It just means that the error is less than what we can measure for that period.

### Example entries for Frequency errors at System start-up

```
16649,77897,1,0,gps0,gps0,34190,-22,-1.44e-11,51.40731016649,77898,1,0,gps0,gps0,34190,-22,-1.
11,52.023643
16649,77900,1,0,gps0,gps0,34190,-22,-1.44e-11,51.348320
16649,77902,1,0,gps0,gps0,34190,-22,-1.44e-11,51.922173
16649,78191,0,0,,,32768,1000000000,1.00e-02,49.073082
16649,78194,0,0,,,32768,1000000000,1.00e-02,49.147850
16649,78196,0,0,,,32768,1000000000,1.00e-02,49.164482
16649,78199,0,0,,,32768,1000000000,1.00e-02,49.222649
16649,78201,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.297508
16649,78203,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.322472
16649,78206,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.230980
16649,78207,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.380699
```

### cron.log (Cron log entries)

fcrontab[2441]: installing file /tmp/fcr-9TuBXK for user root

- Per Paul Myers, this entry appears to be related to cron initially starting-up as part of system boot-up (it was asserted after a unit was rebooted, in addition to other log entries associated with normal system boot-up.

---

## Cron log reports “[RESTART] Restarting initiated for snmpsad” followed by “[SUCCESS] Successfully restarted snmpsad”

- These two log entries are an indication that only the SNMPSAD subagent was restarted – not the SNMPd agent being restarted because our “watchdog” detected snmpsad wasn’t running.
- If snmpsad crashes and needs to be reset, non-spectracom mibs will still be fine, but the spectracom mibs won’t be able to respond until snmpsad has successfully restarted.
- snmpsad is being updated in software version 5.2.0 to allow SNMP to be updated to a newer version. If these two entries are periodically being asserted, it’s recommended to update to at least version 5.2.0.

---

## daemon.log (daemon log entries)

- log entries for daemons (such as NTP, SNMP, XINETd, etc)
- this is a linux OS log – not a Spectracom log
- This log may not be wiped with a “clean logs”

### A) Example daemon.log entries for xinetd

- Refer to: <http://linux.die.net/man/5/xinetd.log>

1. xinetd[3637]: warning: can't get client address: Connection reset by peer  
<http://forum.sp.parallels.com/threads/xinetd-16263-warning-cant-get-client-address-connection-reset-by-peer.71361/>  
“It is normal warning that the address of remote server could not be known”

#### Suggestions if this entry is often being intermittently asserted:

- Review the kern.log to see if eth0 is set to 10MB/half duplex (because it can’t negotiate with a switch that is hard-set) as shown in the example entry below. This connection issue can “silent lockup” of the ETX module, (until unit is rebooted) especially in periods of heavier than usual network traffic

**8139too 0000:00:06.0 eth0: link up, 10Mbps, half-duplex, lpa 0x0000**

---

### B) Example daemon.log entries for SNMP (associated with SNMPd or SNMPSAD)

- Refer to the “SNMP” section of this document for more info on these error messages.
- Recommended to update software to v5.2.0 or higher to upgrade NET-SNMP to newer version  
**Note:** daemon log records only “WARNING” or error messages about SNMP. Refer to the Journal log for entries showing SNMPd being stopped and started (normal operation).

#### Wrong netlink

**netlink** - communication between kernel and user space (AF\_NETLINK)

Netlink is used to transfer information between kernel and user-space processes. It consists of a standard sockets-based interface for user space processes and an internal kernel API for kernel modules. The internal kernel interface is not documented in this manual page. There is also an obsolete netlink interface via netlink character devices; this interface is not documented here and is provided only for backward compatibility.

#### snmpd[2065]: Wrong netlink message type 3

- Refer to SR 4958/SR 5490 in SAP (customer was running v5.3.0)

## SNMP Build Errors

“Error building ASN.1 representation, SNMP Build Unknown Failure, RFC1213-MIB Messages” or

“send response: Error building ASN.1 representation (wrong type in snmp\_realloc\_rbuild\_var\_op: 199)”

- This is a known condition in RFC-1213
- Doesn't affect operation of SNMP
- Refer to <http://www.teragauge.com/index.php/support/knowledge-base/19-kb-troubleshooting/53-kb-tg-snmp-syslog-error-msg>

#### **SNMP already started (trying to enable SNMP while it's already running)**

**/etc/init.d/snmpd[22014]: WARNING: snmpd has already been started**

- Asserted when trying to start SNMP when its already enabled (using the servset 7 on command to enable SNMP, not realizing the browser shows its already running)

#### **SNMP already stopped (trying to disable SNMP while it's already stopped)**

**/etc/init.d/snmpd[8047]: WARNING: snmpd is already stopped**

- Asserted when trying to stop SNMP when its already disabled (using the servset 7 off command to enable SNMP, not realizing the browser shows its already disabled)

**/etc/init.d/snmpsd[29156]: WARNING: snmpsd is already stopped**

- Asserted when trying to stop SNMP when its already disabled (using the servset 7 off command to enable SNMP, not realizing the browser shows its already disabled)

#### **Superuser entry**

**/etc/init.d/snmpd[14810]: snmpd: superuser access required**

- Oleg believes this entry was likely asserted in a customer's log when a user tried to manually start/stop SNMP in “/etc/init.d” (instead of using either the browser or CLI). Note that it's unlikely there will be an associated log entry asserted in the journal log for this attempted situation.
- Since a user won't have root access, they can't issue any linux commands to stop or restart Services such as SNMP.

??

Spectracom-CLK2 /etc/init.d/snmpd[22442]: start-stop-daemon: no matching processes found

Spectracom-CLK2 /etc/init.d/snmpd[21939]: start-stop-daemon: no matching processes found

---

### **C) Example daemon.log entries for NTPD**

Spectracom-CLK2 /etc/init.d/ntp[3108]: start-stop-daemon: no matching processes found

NTP stopping: Spectracom-CLK2 /etc/init.d/ntp[14530]: status: stopping (NTP was stopped)

ntp: unknown function `kill' (followed by) status: starting (indicates NTP was automatically restarted)



---

**runtime config from ::1 rejected: request contains an unprintable character: 20**

- Refer to Salesforce Case 287361
- CF card was at 5.7.1 at one time before updating to 5.8.9 (but diskhealth ok)

## error\_log (Apache HTTP Error log entries)

- These are error log entries from Apache2 ( `/var/log/apache2/error.log`)
- For **general info** on this log, refer to: <http://httpd.apache.org/docs/2.2/logs.html>
- For **status codes** (\*such as "200-OK") refer to: [https://www.rackspace.com/knowledge\\_center/article/interpreting-common-status-codes-in-web-logs](https://www.rackspace.com/knowledge_center/article/interpreting-common-status-codes-in-web-logs)
- This is the place where Apache httpd will send diagnostic information and record any errors that it encounters in processing requests. It is the first place to look when a problem occurs with starting the server or with the operation of the server, since it will often contain details of what went wrong and how to fix it.
- Added to the log bundle in software version 5.2.1 (I believe)
- Starts with ".log.1" as the file extension instead of just ".log" like the other log files
- Can't view them in the browser. View this log via CLI or from a log capture file

### Log entry format

- Example log entry `[Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test`

### Error log components

1. **The first part of the log entry** is the date and time (server time) when the event occurred. Apart from just being informative, that time can be useful for looking for entries in other logs at the same time. In this case, check the access log to see the full URL that the web client tried to visit. If it was an error that indicated a module had trouble talking to a database, then look in the database server's logs at the same time to see what prevented the connection from happening.
2. **The next part**, "[error]", describes the level of the alert. This will often be "error", but sometimes other levels will indicate that the message logged is just a warning, or it may represent a critical error that caused the web server to shut down or fail to start.
3. **The next part**, "[client 80.154.42.54]", shows the source of the error. In this case the source is a web client, so the visitor's IP address was logged.
4. **The last part of the log entry is the error itself:**

### D) Normal error\_log entries for logging out of spadmin account

```
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlog- authmethod is currently (null) (for /Users/logout), referer: http://10.2.100.176/  
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlog- authtype is currently Pamacea (for /Users/logout), referer: http://10.2.100.176/  
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlog- authmethod is currently (null) (for /toolsb) /contact), referer: http://10.2.100.176/  
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlog- authtype is currently Pamacea (for /tools/contact), referer: http://10.2.100.176/
```

### E) Normal error\_log entries for login to spadmin account

```
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlog- authmethod is currently (null) (for /Home), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlog- authtype is currently Pamacea (for /Home), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlog- authmethod is currently (null) (for /users/login), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlog- authtype is currently Pamacea (for /users/login), referer: http://10.2.100.176/tools/contact  
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlog- authmethod is currently (null) (for /users/login), referer: http://10.2.100.176/users/login  
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlog- authtype is currently Pamacea (for /users/login), referer: http://10.2.100.176/users/login
```

## F) Error\_log entries from a SecureSync exhibiting error 500 messages when logging in

```
enable, referer: https://10.82.133.149/auth/login.html?target=/cgi-  
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Not processing line, referer:  
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value  
then, referer: https://10.82.133.149/auth/login.html?target=/cgi-  
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value  
then, referer: https://10.82.133.149/auth/login.html?target=/cgi-  
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Premature end of script headers: StatusConfig.cgi, referer:  
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authmethod is currently (null) (for  
/spec500err.html), referer: https://10.82.133.149/auth/login.html?target=/cgi-  
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=  
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authtype is currently Pamacea (for  
/spec500err.html), referer: https://10.82.133.149/auth/login.html?target=/cgi-  
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
```

## G) “RSA server certificate CommonName (CN) `Spectracom' does NOT match server name!”

- Indicates web browser Security Settings may be set too high. Try lowering the settings to the lowest value and then login again.
- May need to replace the default HTTPS certificate with a new one using values particular to the network.

---

## events.log (Events log entries)

**All Power Inputs Detected:** The SecureSync can be configured for AC and/or DC input power. This entry indicates that applicable power has been detected on all available inputs.

---

**“Power or Configuration Fault”** (along with either **“Timing System Software Error”** or **Timing System Hardware Error”**)

- Refer to Salesforce Cases such as: 221716, 219284, 215921, 213323
- Appears to be asserted after a reboot when there is a hardware issue with oscillator/FPGA??
- At least sometimes coupled with **“failed CS\_GetTime (KAD)”** **“Failed HW\_GetTime (probably FPGA failure) (KAD)”** (in **System** log) AND with either **“Timing System Software Error”** or **“Timing System Hardware Error”** (**Events** log)

---

**“1PPS not in Specification”** / **“1PPS Restored to Specification”**

These are events that occur and alarm entries that are asserted. “1PPS not in Specification” occurs if the current TFOM values exceed the user-configurable max TFOM value. When the TFOM falls below Max TFOM, the Restored to Specification event/alarm entry is asserted.

Regarding the “1PPS Not in Specification” alarm, this alarm only occurs if the current TFOM exceeds the user-configurable max TFOM value. The SecureSync going into Holdover mode will not initially and automatically cause the TFOM to increase and exceed the max TFOM value. However, if the unit continues to operate for an extended period of time without any valid input references, the oscillator will begin to drift. As long as the max TFOM is not set to 15, eventually, the max TFOM will be exceeded and the alarm is asserted. The type of oscillator (OCXO or Rubidium) and the setting of max TFOM will determine the typical amount of time in holdover required to exceed the max TFOM.

---

**Frequency Error:** “Frequency Error Detected” indicates either the unit had recently been rebooted, a large oscillator frequency offset was detected (such as changing from one selected input reference to another). It is also asserted when the SecureSync is synced to either NTP or USER and therefore, the oscillator cannot be disciplined to the selected reference.

The frequency error threshold for this alarm to be asserted is oscillator type dependant

**Frequency Error Cleared** indicates the oscillator has relocked after a recent power cycle or has been steered to compensate for a large frequency error. Fractional frequency error is less than  $1 \times 10^{-8}$

---

**Reference Change / Reference Changed to / Reference Change Cleared:** The highest present and valid priority reference that was available was lost, so the next highest present and valid priority was selected.

**Note:** The Reference Change entry is also asserted when the SecureSync goes into Holdover mode (no references currently available).

**Note:** (Starting in software versions 5.0.1 and above), a second entry is also asserted to indicate what references were just selected (example: **SS: Reference changed to Time Ref: gps0 PPS Ref: gps0**). When the SecureSync goes into Holdover mode, the entry will indicate “none” as the selected reference (example: **SS: Reference changed to Time Ref: none PPS Ref: none**)

Q. What does **“Reference Change”** and **“Reference Change (Cleared)”** refer to?

**A.** When the preferred reference is not valid or a preferred valid reference is detected in the priority reference table the system sets a Reference Change bit in a register that tells the system that it needs to change references. After the system changes references that bit is cleared. When these events occur, their respective notifications are displayed in the logs.

Q And their relation to Holdover state?

**A If NO References are available such as GPS or NTP your reference will change to Holdover state until either the holdover time that you have set has expired or until the system detects a valid reference.**

**Reference Change (Cleared):** System entry just to reset the “Reference Change” state. This entry can be disregarded.

---

**In Holdover / No longer in Holdover** (Holdover event)

- Note that in at least software versions 5.3.1 and below, Holdover is an Event (entry in the Events log) instead of being an Alarm (entry in the Alarms log).

Indicates the NTP server lost synchronization to its external reference input and it's using the internal reference oscillator to derive the time outputs. This alarm is classified as a Minor alarm condition. The Holdover mode will continue until the reference is restored, it times out as configured in the System/Holdover page, or the unit NTP server is rebooted/power cycled. If Holdover mode times out, at that time a Time Sync alarm will be asserted.

During the Holdover mode, all outputs remain available to synchronize other devices. This mode is just an alert that the primary input is not available and so the oscillator is being used to provide time outputs. There is no other effect on the operation of the system while in the mode.

“In Holdover” indicates no input references are currently present and valid. The oscillator is in free-run mode. Time is being maintained by the oscillator and is still valid for synchronization. “No longer In Holdover” indicates at least one input reference has been restored, or no input references have been restored and the Holdover period has expired. Time is no longer valid for synchronization.

---

**In Sync / Not In Sync:** “In Sync” indicates SecureSync has at least one present and valid reference to sync with. Time is valid for synchronization. “Not In Sync” indicates SecureSync has no present and valid references to sync with and the Holdover period has elapsed. Time is no longer valid for synchronization.

---

**GPS Antenna Problem / GPS Antenna OK:** Based on measured current draw, “GPS Antenna Problem” indicates the GPS receiver detected the antenna is not connected or there is an open/short in the antenna cable. “GPS Antenna OK” indicates the GPS receiver has detected an expected amount of current draw. So the antenna appears to be connected to the GPS receiver with a good cable connection

---

**The Unit Has Rebooted:** This entry indicates the SecureSync was either power cycled or rebooted via a CLI interface (such as the web browser).

---

**Error entry periodically being asserted “[system] ERROR - KW\_HR\_SetTime returned [rc = 3]”**

- Refer to Salesforce cases 14919 (Dongjin) and 12869 (Open Access, Australia)
- Apparently asserted when NTP input tries to set the KTS time but is not able to.
- Verify the proper configuration of the NTP Peers and NTP Servers tabs.
- Dongjin had the Enable Stratum 0 PPS reference (127.127.22.0 in Expert mode) enabled with a peer configured

---

Failed to report event to NOTD followed by  
Failed to report event to NOTD (GPSD)

- Refer to Salesforce case 20365 (Kaiser)
- Kern log also contained “hda” error messages such as :

Jan 12 18:23:10 cdcntp202 kernel: hda: dma\_intr: status=0x51 { DriveReady SeekComplete Error }  
Jan 12 18:23:10 cdcntp202 kernel: hda: dma\_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=87817,

sector=87817  
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8  
Jan 12 18:23:10 cdcntp202 kernel: end\_request: I/O error, dev hda, sector 87817  
Jan 12 18:23:10 cdcntp202 kernel: hda: dma\_intr: status=0x51 { DriveReady SeekComplete Error }  
Jan 12 18:23:10 cdcntp202 kernel: hda: dma\_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049, sector=88049  
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8  
Jan 12 18:23:10 cdcntp202 kernel: end\_request: I/O error, dev hda, sector 88049  
Jan 12 18:24:37 cdcntp202 kernel: hda: dma\_intr: status=0x51 { DriveReady SeekComplete Error }  
Jan 12 18:24:37 cdcntp202 kernel: hda: dma\_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049, sector=88049

**Email from Paul Myers (13 Jan 2016)** I may have commented on this before keith, but this unit looks like 2 issues. Possibly the mysql database is not working write for some errors, but the 2<sup>nd</sup> errors you point out give me concern the CompactFlash is corrupted or worst case the interface to the CF in hardware is causing errors.

You could reboot and clean and see what happens. OR you could do a clean update. If the errors exist below then you might have a bad CF or ATA CF interface in hardware is bad. Most likely CF though.

Jan 12 18:23:10 cdcntp202 kernel: hda: dma\_intr: status=0x51 { DriveReady SeekComplete Error }

---

**Failed to report event to NOTD (KAD)** followed by

**Failed to read oscillator frequency error from KTS (KAD)**

- Refer to Salesforce case 18880 (RMA found SecureSync had a bad OCXO osc)

---

**The Unit Has Rebooted:** This entry indicates the SecureSync was either power cycled or rebooted via a CLI interface (such as the web browser)

---

**SAASM rceiver-related log entries in the Events log (even though a SAASM receiver is not installed)**

**specific examples of log entries that were observed:**

- “The SAASM Key will not Expire Soon”
  - “The SAASM Key is Valid”
- This condition should not be observed in at least version 5.4.5 or above.
  - This was a software issue that was addressed sometime before version 5.4.5 release (not sure which earlier version actually fixed it, but it was fixed before v5.4.5 was released)

**Email from Paul Myers (26 Oct 16)** There was a bug which caused SAASM event entries to be logged because they were not inhibited. This was corrected in some release since then. Updating to 5.4.5 or better yet 5.5.0 would fix that.

---

## (journal.log) Journal log entries

**Note:** entries vary based on whether changes made in classic interface or newer (black/charcoal interface)

- Which *interface* was the config change made (“Entity” field in the browser)?
- **[frontpanel]:** changes made via front panel

| Id | Date               | Entity       | Message                                     |
|----|--------------------|--------------|---------------------------------------------|
| 6  | Aug 01<br>21:45:35 | [frontpanel] | requests DHCP lease for eth0 to be renewed. |

- **[spadmin]:** Changes made via the spadmin account (Will only be seen with changes made using classic interface)

| Id | Date               | Entity    | Message                                                          |
|----|--------------------|-----------|------------------------------------------------------------------|
| 42 | Sep 11<br>15:10:35 | [spadmin] | set DNS for eth1 to .                                            |
| 41 | Sep 11<br>15:10:35 | [spadmin] | set DNS for eth1 to 10.1.1.26.                                   |
| 40 | Sep 11<br>15:10:33 | [spadmin] | no changes applied for IPv4 Default Gateway for eth1 to 0.0.0.0. |

- **[WEB]:** changes made via the web browser

| Id | Date               | Entity | Message                                                |
|----|--------------------|--------|--------------------------------------------------------|
| 39 | Sep 10<br>18:01:40 | [WEB]  | Changed port settings for eth1 to autoneg on (spadmin) |

- **[webUI]:** changes made via the web browser

| Id | Date               | Entity  | Message                       |
|----|--------------------|---------|-------------------------------|
| 38 | Sep 10<br>18:01:40 | [webui] | set port for eth1 to enabled. |

- **[root]:** changes made automatically by the system

| Id | Date               | Entity | Message                                        |
|----|--------------------|--------|------------------------------------------------|
| 27 | Aug 06<br>13:46:02 | [root] | SNMP agent has been started.                   |
| 24 | Aug 06<br>13:45:45 | [root] | SNMP agent inhibited from starting up on boot. |

---

Which *user account* made the change (not applicable to changes made via the front panel keypad)

- **[spadmin]:** Changes made via the spadmin account (Will only be seen with changes made using classic interface)

| Id | Date               | Entity    | Message                                                          |
|----|--------------------|-----------|------------------------------------------------------------------|
| 42 | Sep 11<br>15:10:35 | [spadmin] | set DNS for eth1 to .                                            |
| 41 | Sep 11<br>15:10:35 | [spadmin] | set DNS for eth1 to 10.1.1.26.                                   |
| 40 | Sep 11<br>15:10:33 | [spadmin] | no changes applied for IPv4 Default Gateway for eth1 to 0.0.0.0. |

- **[frontpanel]:** These entries wont report a user account, as accounts don't apply to the front panel Keypad.
- **[WEB]:** these entries indicate user account at the end of the entry:  
"Changed port settings for eth1 to autoneg on (**spadmin**)"
- **[webUI]:** these entries do not indicate which user account made the change (in at least versions 5.8.5 and below)  
"No Authorization mode found. Defaulting to Password and Keys."

(Applicable to at least versions 5.8.5 to 5.1.2- newer browser) Notes about having BOTH **[WEB]** and **[webUI]** journal log entries asserted (the main difference between them is one reports user account info, while the other one doesn't report user account)

**Per Ron Dries (11 Sept 2019)** "Based on this. it appears there is a logging difference that would need to be looked at)

- Refer to Salesforce Case **208350** (for New York City PD)
- Refer to **JIRA ticket SSS-688** (created Sept 2019)

---

## Specific example Journal log entries (entries may be from either ClassicUI or newer browser)

### A) Entries associated with network settings

#### 1. DHCP

set DHCP for eth0 to enabled.

set DHCP for eth0 to disabled.

requests DHCP lease for eth0 to be released: (in at least versions 5.3.0 and above), only asserted when DHCP is enabled and user performs a release (not asserted when DHCP is disabled)

requests DHCP lease for eth0 to be renewed (in at least versions 5.3.0 and above), only asserted when DHCP is enabled and user performs a renew (not asserted when DHCP is disabled)

#### 2. Setting Gateway address

Nov 30 16:02:55 Spectracom Spectracom: [frontpanel] setting IPv4 Default Gateway to 10.0.50.1.

Nov 30 16:02:55 Spectracom Spectracom: [frontpanel] setting IPv4 Default Gateway for eth0 to 10.0.50.1.

Nov 30 16:02:56 Spectracom Spectracom: [frontpanel] requests DHCP lease for eth0 to be released.

Nov 30 16:03:03 Spectracom Spectracom: [frontpanel] requests DHCP lease for eth0 to be renewed.

DHCP lease for eth0 to be released and DHCP lease for eth0 to be renewed.: (per Stuart 6 Dec 2018) though it appears a user did something on the front panel to assert these release/renew entries, these two actions are performed automatically by the system each time a gateway address config change occurs



---

## B) Entries associated with manually setting the time

[frontpanel] Set Time for User Reference 0 in slot 0 to HR (0) Time: 2012 38 3:29:40 {500000000}: Indicated a user had manually changed the System Time to the value at the end of this log entry. The very beginning of the entry also indicates if the System Time was changed by a user via the web browser or by the front panel keypad.

“[spadmin] Changed Constellation Selection for GPS Reference 0 in slot 0 from GR (0) ConstellationSelection: (3) : ^IGPS ^IGLONASS to GR (0) ConstellationSelection: (1) : ^IGPS:” :

## C) Reboots and Halts

- Update version 5.4.5 added journal entries for reboots and halt commands issued in CLI interface.

## D) GNSS receiver constellation selection was changed by a user.

Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true XO\_GetDac 0 (KTSAL)

Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL\_Get - Label(oscillator\_ca\_dac0) - devindex(0) - index(4294967295) (WEB)

Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true XO\_GetDac 0 (KTSAL)

| Event           | Alarm                  | Oscillator                                                                                                 | GPS Qualification | NTP | Journal | Authentication | Update | Timing | System |
|-----------------|------------------------|------------------------------------------------------------------------------------------------------------|-------------------|-----|---------|----------------|--------|--------|--------|
| Jul 17 18:36:27 | Spectracom spectracom: | [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB) |                   |     |         |                |        |        |        |
| Jul 17 18:36:27 | Spectracom spectracom: | [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)                           |                   |     |         |                |        |        |        |
| Jul 17 18:20:43 | Spectracom spectracom: | [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB) |                   |     |         |                |        |        |        |
| Jul 17 18:20:43 | Spectracom spectracom: | [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)                           |                   |     |         |                |        |        |        |
| Jul 17 18:20:10 | Spectracom spectracom: | [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB) |                   |     |         |                |        |        |        |
| Jul 17 18:20:10 | Spectracom spectracom: | [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)                           |                   |     |         |                |        |        |        |

### Email from Dave Sohn (6/20/12)

There isn't any issue with the unit. This is just a reporting bug. The system is in the background querying the DAC value for some reporting, but that isn't a valid call for a Rubidium unit, so there is an error. There is no effect on operation, and that error doesn't mean there is any problem with the unit. You can enter a Mantis case for it, and we will discuss it in SW CCB.

(8/31/12 KW) Update – the fix for this issue should be in the version 4.8.7 release

---

## E) Journal logs entries related to watchdog being enabled (applicable to v5.8.9 and above)

| Id | Date            | Entity   | Message               |
|----|-----------------|----------|-----------------------|
| 29 | May 04 12:44:22 | watchdog | functionality enabled |

---

## F) Journal log entries related to SNMP

Reset SNMP configs via button in newer black browser

[WEB] Performed SNMP restore configuration function (admin): user pressed the button to reset just the SNMP configs

### Starting (Enabling) SNMP

#### 1. Via newer black interface web browser

In at least version 5.2.0, no log entry is asserted when user enables SNMP via the black browser (Refer to Mantis case 2997)

## 2. Via classic interface web browser

(**Note:** both entries below are asserted each time)

[spadmin] SNMP agent configured to start up on boot. SNMP was enabled by a user. The next time the unit is booted-up, SNMP will be automatically started while in this state.

[spadmin] SNMP agent has been started. SNMP daemon is now running.

## Stopping (Disabling) SNMP Service

### 1. Via newer black interface web browser

(Note: only the one entry below is asserted each time)

[WEB] Stopped SNMP services (spadmin): user disabled SNMP via the new browser

### 2. Via classic interface browser

(Note: both entries below are asserted each time)

[spadmin] SNMP agent inhibited from starting up on boot. SNMP was disabled by a user. The next time the unit is booted-up, SNMP will not be automatically started while it's in this state.

[spadmin] SNMP agent has been shut down. SNMP daemon is now stopped.

---

## **Kern.log (Kernel Log entries)**

Kernel Entries and other indicating potential software/hardware issues happening (such as a potential ETX failing, SNMP crashing or an issue with the CF card)

- Consists of log entries associated with the Linux OS (not “Spectracom” log entries)
- “Linux kernel map” added in software update version 5.2.0 for improved diagnostics
  - Maps memory locations
  - Example related kernel entries
    - “Inspecting /boot/System.map-3.8.13-gentoo”
    - “Cannot find map file.”

**Segfault entries:** segfault indicates a processing error has occurred.

---

### 1. “kernel: perf: interrupt took too long”/,”lowering kernel.perf\_event\_max\_sample\_rate to” entries

**Apr 29 15:53:54** 10 kernel: perf: interrupt took too long (2515 > 2500), lowering kernel.perf\_event\_max\_sample\_rate to 79000

**Apr 29 16:01:08** 10 kernel: perf: interrupt took too long (3163 > 3143), lowering kernel.perf\_event\_max\_sample\_rate to 63000

**Apr 29 16:17:57** 10 kernel: perf: interrupt took too long (3966 > 3953), lowering kernel.perf\_event\_max\_sample\_rate to 50000

- First observed by Keith in 5.8.9
- (5 May 2020) Ryan Johnson stated during a call that Engineering had also observed these entries and they are not an indicator of a problem (he said the entries have been observed with both 1<sup>st</sup> Gen and 2<sup>nd</sup> Gen ETX modules installed).

---

### 2. Kernel lockup with “page allocation stalls” and “out of memory manager” - due to issue with TACACS (associated with versions 5.8.5 and 5.8.5)

**Example kern.log entry:** “Apr 27 05:03:55 atl1r033-ntp03 kernel: syslogd: page allocation stalls for 14471ms, order:0, mode:0x1c200ca(GFP\_HIGHUSER\_MOVABLE|\_\_GFP\_WRITE), nodemask=(null)”

- Refer to SF Case 193787 and JIRA Ticket SSS-640
- Refer also to the TACACS troubleshooting info in this document
- Associated with “memory leak” on 2<sup>nd</sup> gen ETX, version 5.8.4 and TACACS
- seen with version 5.8.4 /2<sup>nd</sup> gen ETX module installed)
- Expected to be fixed in v5.8.6

Delta Airlines observed a v5.8.4 Kernel lockup (with 2nd gen ETX module installed) – “Call Trace” “page allocation stalls” and “out of memory manager” entries- due to issue with TACACS

The unit locked up. Cant login and not responding to NTP. They have power cycled which has restored connection.

**Email from Ryan Johnson to Scott Z** I discussed this with Stuart, and not to downplay the issue at all but this particular case looks to be easier to point to a cause than the other mystery kernel crashes that we’ve seen before. This lockup is actually

more similar to the recent VelaSync issue where a particular software process (in this case TACACS) is leaking memory to the point where eventually it's all used up.

It may not be a simple fix however as TACACS is a fairly complex mechanism. Stuart did request additional information on how the customer is using it to hopefully help us be able to recreate the issue. Any use-case like information that you can extract from the customer would be helpful.

**Per Ryan Johnson (6 May 2019)** This is a new issue – we were unaware of it as well. At this point I can't commit to a timeline for resolution other than that it almost certainly will *not* be in the next release (5.8.5) as the scope for that is small and already frozen. We still need more information on the cause before understanding how we would potentially fix.

---

### 3. 8139too.ko

- Per Ron Dries, Not an issue if a 2<sup>nd</sup> generation ETX module is installed

```
spadmin@4 /lib/modules/4.14.34-gentoo-x64 $ find /lib/modules/ -name 8139too.ko
/lib/modules/4.14.34-gentoo/kernel/drivers/net/ethernet/realtek/8139too.ko
```

```
spadmin@4 /lib/modules/4.14.34-gentoo-x64 $ find /lib/modules/ -name e100.ko
/lib/modules/4.14.34-gentoo-x64/kernel/drivers/net/ethernet/intel/e100.ko
/lib/modules/4.14.34-gentoo/kernel/drivers/net/ethernet/intel/e100.ko
```

**Email from Ron Dries (3 Dec 2018)** The 8139too error is not an issue. The newer (64 bit, instead of 32 bit) ETX module does not use it and it appears he has the newer ETX module.

### “kernel: net\_ratelimit: callbacks suppressed” entries (log entries to syslog server being suppressed)

- Indicates log entries to be sent to syslog server are being suppressed to prevent overloading the syslog server
  - This was observed with SF case 126253 where there were many of these kern.log entries generated over a short period of time, with many entries also in the snmp.log

```
Feb 6 20:44:03 w0001-ntp-1200a kernel: net_ratelimit: 21 callbacks suppressed
Feb 6 20:44:13 w0001-ntp-1200a kernel: net_ratelimit: 19 callbacks suppressed
Feb 6 20:44:18 w0001-ntp-1200a kernel: net_ratelimit: 187 callbacks suppressed
Feb 6 20:44:23 w0001-ntp-1200a kernel: net_ratelimit: 216 callbacks suppressed
Feb 6 20:44:28 w0001-ntp-1200a kernel: net_ratelimit: 75 callbacks suppressed
Feb 6 20:44:33 w0001-ntp-1200a kernel: net_ratelimit: 1 callbacks suppressed
Feb 6 20:44:46 w0001-ntp-1200a kernel: net_ratelimit: 1 callbacks suppressed
Feb 6 20:44:52 w0001-ntp-1200a kernel: net_ratelimit: 23 callbacks suppressed
```

I found the note below at <https://serverfault.com/questions/277009/what-does-net-ratelimit-44-callbacks-suppressed-mean-on-a-linux>

*“this “callbacks suppressed” message implies it suppressed a bulk of 44 syslog messages. This is an attempt to avoid loading your syslog logging path.”*

---

### TCPDump/packet sniffer related entries

#### promiscuous mode

```
Device eth0 entered promiscuous mode
kernel: device eth0 left promiscuous mode
```

From <http://www.linuxquestions.org/questions/linux-security-4/kernel-device-eth0-entered-promiscuous-mode-756884/>

“Promiscuous mode means a packet sniffer instructed your ethernet device to listen to all traffic. This can be a benign or a malicious act, but usually you will know if you run an application that provides you with traffic statistics (say ntop or vnstat) or an IDS (say Snort, Prelude, tcpdump or wireshark) or Something Else (say a DHCP client which isn't promiscuous mode but could be identified as one).

---

## Kernel log entries associated with the KTS driver unloading (likely due to loss of 10 MHz to KTS).

- pps pps0: tsyncpci PPS source unregistered
- Spectracom TSync Timing Board removed

**Note:** Refer to ([\\*\\*system.log entries \(and MySQL database\)](#)) in this document for more info on how the loss of 10 MHz from the oscillator can assert these entries due to its adverse affect on KTS.

---

## Eth0 at 10/half (due to switch being hard-set) can cause ETX lock-ups

- 10/half in a busy network can cause a watchdog reset of the ETX (indicated in the kernel log):
- Set the switch to auto-negotiate to prevent this condition

```
14 16:04:31 Spectracom kernel: -----[ cut here ]-----
Jun 14 16:04:31 Spectracom kernel: WARNING: CPU: 0 PID: 0 at net/sched/sch_generic.c:303 dev_watchdog+0x199/0x1b0()
Jun 14 16:04:31 Spectracom kernel: NETDEV WATCHDOG: eth0 (8139too): transmit queue 0 timed out
Jun 14 16:04:31 Spectracom kernel: Modules linked in: e1000e(O) e100 8139too mii tsyncpci(O)
Jun 14 16:04:31 Spectracom kernel: CPU: 0 PID: 0 Comm: swapper Tainted: G      O  4.0.5-gentoo #1
Jun 14 16:04:31 Spectracom kernel: Hardware name: /AMD-GX3, BIOS 6.00 PG 11/04/2008
Jun 14 16:04:31 Spectracom kernel: dec09f58 dec09f58 dec09f2c c133d015 dec09f48 c10330c5 0000012f c128ab49
Jun 14 16:04:31 Spectracom kernel: dee66000 00000000 ffff88a dec09f60 c1033116 00000009 dec09f58 c141d664
Jun 14 16:04:31 Spectracom kernel: dec09f74 dec09f94 c128ab49 c1419d6e 0000012f c141d664 dee66000 e082fa9c
Jun 14 16:04:31 Spectracom kernel: Call Trace:
Jun 14 16:04:31 Spectracom kernel: [
```

---

## “hda” Kernel log entries associated with a failing/bad CF card

```
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError },
LBAsect=1583721, sector=1583721
Mar 23 14:55:34 Spectracom kernel: hda: possibly failed opcode: 0xc8
Mar 23 14:55:34 Spectracom kernel: blk_update_request: I/O error, dev hda, sector 1583721
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Mar 23 14:55:34 Spectracom kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError },
LBAsect=1583721, sector=1583721
Mar 23 14:55:34 Spectracom kernel: hda: possibly failed opcode: 0xc8
Mar 23 14:55:34 Spectracom kernel: blk_update_request: I/O error, dev hda, sector 1583721
```

Mar 23 14:55:34 Spectracom kernel: hda: dma\_intr: status=0x51 { DriveReady SeekComplete Error }  
Mar 23 14:55:34 Spectracom kernel: hda: dma\_intr: error=0x44 { DriveStatusError UncorrectableError },  
LBAsect=1583721, sector=1583721  
Mar 23 14:55:34 Spectracom kernel: hda: possibly failed opcode: 0xc8  
Mar 23 14:55:34 Spectracom kernel: blk\_update\_request: I/O error, dev hda, sector 1583721  
Mar 23 14:55:44 Spectracom kernel: spurious 8259A interrupt: IRQ7.

---

## Ethernet driver issues related entries

- Version 5.3.0 updated the Ethernet driver to improve its performance.
  - From the release notes: “Gigabit Ethernet Option Card: Updated Gigabit Ethernet driver to version 3.1.0.2”

Apr 7 21:22:15 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_UP): eth0: link is not ready  
Apr 7 21:23:23 RP5NTP kernel: 8139too 0000:00:06.0 eth0: link up, 100Mbps, full-duplex, lpa 0xC1E1  
Apr 7 21:23:23 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_CHANGE): eth0: link becomes ready  
Apr 7 21:38:46 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_UP): eth1: link is not ready  
Apr 7 21:38:49 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Apr 7 21:38:49 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_CHANGE): eth1: link becomes ready  
Apr 7 21:43:25 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_UP): eth2: link is not ready  
Apr 7 21:44:13 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_UP): eth3: link is not ready  
Apr 7 22:25:05 RP5NTP kernel: e1000e: eth2 NIC Link is Up 100 Mbps Full Duplex, Flow Control: None  
Apr 7 22:25:05 RP5NTP kernel: e1000e 0000:04:00.0 eth2: Link Speed was downgraded by SmartSpeed  
Apr 7 22:25:05 RP5NTP kernel: e1000e 0000:04:00.0 eth2: 10/100 speed: disabling TSO  
Apr 7 22:25:05 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_CHANGE): eth2: link becomes ready  
Apr 29 02:07:18 RP5NTP kernel: e1000e: eth2 NIC Link is Down  
Apr 29 02:11:43 RP5NTP kernel: e1000e: eth2 NIC Link is Up 100 Mbps Full Duplex, Flow Control: None  
Apr 29 02:11:43 RP5NTP kernel: e1000e 0000:04:00.0 eth2: Link Speed was downgraded by SmartSpeed  
Apr 29 02:11:43 RP5NTP kernel: e1000e 0000:04:00.0 eth2: 10/100 speed: disabling TSO  
Apr 29 02:11:43 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_CHANGE): eth2: link becomes ready  
May 12 16:47:48 RP5NTP kernel: 8139too 0000:00:06.0 eth0: link down  
May 12 16:51:13 RP5NTP kernel: 8139too 0000:00:06.0 eth0: link up, 100Mbps, full-duplex, lpa 0xC1E1  
May 12 16:51:13 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_CHANGE): eth0: link becomes ready  
May 21 15:08:01 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
May 21 15:08:01 RP5NTP kernel: IPv6: ADDRCONF(NETDEV\_CHANGE): eth1: link becomes ready  
May 21 15:08:11 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
May 22 06:11:18 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
May 22 23:58:01 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
May 24 14:03:39 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Jun 30 23:59:59 RP5NTP kernel: Clock: inserting leap second 23:59:60 UTC  
Sep 24 00:20:24 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Sep 24 00:46:08 RP5NTP last message repeated 2 times  
Sep 24 00:46:19 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Dec 17 20:52:54 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Dec 17 20:53:05 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Dec 19 02:30:16 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Dec 23 07:19:05 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Dec 31 19:37:05 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Dec 31 19:37:15 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Jan 6 21:46:12 RP5NTP kernel: e1000e: eth2 NIC Link is Up 100 Mbps Full Duplex, Flow Control: None  
Jan 6 21:46:12 RP5NTP kernel: e1000e 0000:04:00.0 eth2: Link Speed was downgraded by SmartSpeed  
Jan 6 21:46:12 RP5NTP kernel: e1000e 0000:04:00.0 eth2: 10/100 speed: disabling TSO  
Jan 14 17:53:26 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Jan 14 20:47:02 RP5NTP last message repeated 2 times  
Jan 14 20:47:13 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Feb 6 18:44:00 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Feb 10 17:48:13 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Feb 11 17:47:28 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Feb 11 17:47:38 RP5NTP last message repeated 2 times  
Feb 12 20:11:34 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Feb 12 20:11:45 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Feb 16 01:57:20 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None  
Feb 18 18:26:18 RP5NTP kernel: e1000e: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control:

```

Feb 18 20:26:37 RP5NTP kernel: -----[ cut here ]-----
Feb 18 20:26:37 RP5NTP kernel: WARNING: at net/sched/sch_generic.c:254 dev_watchdog+0x204/0x210()
Feb 18 20:26:37 RP5NTP kernel: Hardware name:
Feb 18 20:26:37 RP5NTP kernel: NETDEV WATCHDOG: eth1 (e1000e): transmit queue 0 timed out
Feb 18 20:26:37 RP5NTP kernel: Modules linked in: e1000e(O) e100 tsyncpci(O) pps_core 8139too
Feb 18 20:26:37 RP5NTP kernel: Pid: 0, comm: swapper Tainted: G      O 3.8.13-gentoo #1
Feb 18 20:26:37 RP5NTP kernel: Call Trace:
Feb 18 20:26:37 RP5NTP kernel: [

```

---

## PREEMPT (likely included in conjunction with “Call Trace” “oops”, “tainted”, “bug” entries)

- Refer also to “Preempt” in this document for more info.
- Preempt is a function that can optionally be enabled in a linux kernel. Our Engineers found references that this function being enabled can cause issues with the OS.
- Software update Version 5.4.0 disabled/turned-off preempt in the linux kernel as a potential fix to these various lockup/hanging issues/kernel log error messages.

## Oops

- Example log below (This log was from a SecureSync that kept locking up- Robert Jelinek/Chris Johnston with PDT partners)

```

spadmin@setimex1 ~ $ dmesg|tail -40
[252021.702178] BUG: unable to handle kernel NULL pointer dereference at (null)
[252021.702499] IP: [

```

---

## Front panel Serial “Console” port is not responding.

---

## SNMPD related entries

### Example Kernel logs showing SNMPd crashed

- (refer to the SNMP section of this document for more info. Note the exact info in the segfault entries may vary.

```
kernel: snmpd[3710]: segfault at 17 ip b76ad597 sp bfc49a30 error 4 in libnetsnmpagent.so.25.0.1[b768e000+67000]
kernel snmpd[1841]: segfault at 17 ip b7701597 sp bfd8d740 error 4 in libnetsnmpagent.so.25.0.1[b76e2000+67000]:
```

Review the kernel log (kern.log) in the log bundle for the following type entries that point to likely issues occurring with Eth0 (all of these entries were asserted on the same day at the same second). Dave Sohn agreed these indicate likely ETX issue.

```
Sep 30 21:38:21 ntp16 kernel: WARNING: at net/sched/sch_generic.c:254 dev_watchdog+0x204/0x210()
kernel: Hardware name:
kernel: NETDEV WATCHDOG: eth0 (e100): transmit queue 0 timed out
kernel: Modules linked in: e1000e(O) 8139too tsyncpci(O) e100 pps_core
kernel: Pid: 17577, comm: sudo Tainted: G      O 3.8.13-gentoo #1
kernel: Call Trace:
kernel: [
```

---

### “LM90” Register read failed log entries (temperature sensor)

- Associated with software versions 5.3.0 and above
- Fixed in update version 5.7.0 (June 2017). Changed the speed of a “SMBUS” monitoring bus on the ETX module.

```
Jun  1 23:21:30 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun  1 23:21:30 s15u1clk kernel: lm90 0-004c: Register 0x19 read failed (-5)
Jun  2 13:06:32 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun  2 13:06:32 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
Jun  6 11:06:33 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun  6 11:06:33 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
```



```
Jun 8 10:08:27 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun 8 10:08:27 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
Jun 8 10:37:27 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x40)
Jun 8 10:37:27 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
```

**Per Paul Myers (20 Jun 16)** The LM90 I2C device is a I2C device driver temp sensor read. This is not uncommon failure in servers for reading I2C temp devices. I am assuming it is intermittent failure to read a temp sensor.

**Per Ron Dries (24 Sept 15)** The lm90 logs have been seen before, I believe its related to reading the temperature from the ETX and CPU.

---

### Kernel logging error “i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)”

Example entry: Jun 2 13:06:32 s15u1clk kernel: i2c i2c-0: **not master in state address** (addr=0x99, len=1, status=0x41)

- Fixed in update version 5.7.0 (June 2017). Changed the speed of a “SMBUS” monitoring bus on the ETX module.

---

### Potential Pipe software command issue (unofficially referred to as the “Verizon issue”)

- Observed by Verizon Wireless and several others (Verizon Salesforce cases 17095 and 16898)
- Review the kernel log (kern.log) in the log bundle for the following type entries (especially “invoked oom-killer:” “segfault” “call trace” “bug”, “inode”, “oops” and “tainted” entries). Note: all of these entries below were asserted on the same day at the same second.
- Update version 5.2.1 (Apr 2015) updated the linux kernel from versions 3.17.7 to 3.18.11 as a potential fix to this kernel software issue.
- This likely software issue is causing browser and SSH to stop working and other functions to stop after kernel crashes occur (sometimes, other functions such as cron and oscillator logs don’t

perfmond.sh invoked oom-killer: gfp\_mask=0x201da, order=0, oom\_score\_adj=0

**Note: “invoked oom-killer” will indicate what was daemon invoked this linux function that is used to try to stop things to free up some memory, due to low memory being available. For example:**

```
kalarmd invoked oom-killer: gfp_mask=0x201da, order=0, oom_score_adj=0
Apr 9 03:46:41 MEY-MNC02 kernel: CPU: 0 PID: 6149 Comm: kalarmd Tainted: G B D O 3.17.7-gentoo #1

oom_kill_process+0x1be/0x320
out_of_memory+0x256/0x290
```

This issue SHOULD be fixed in the version 5.2.1 update. (still being observed in 5.2.1)

### Symptoms that may be observed when this condition occurs

**Reboot** commands may not work due to processes being hung up.

Web browser not accessible functioning

SNMP stops responding.

Serial console port not responding.

Ntpdate command and ntp synchronization of clients failing.

Front panel LCD/keypad not responsive.

**Note:** These words above are potential indications of the pipe software issues with at least v5.1.7 and below (5.1J is a beta for potential fix, with the same changes being added to v5.2.0 (Feb, 2015) as a potential fix.

```
kernel: BUG: unable to handle kernel NULL pointer dereference at 00000028
kernel: IP: [<00000028>] 0x27
kernel: *pde = 00000000
kernel: Oops: 0000 [#1] PREEMPT
kernel: Modules linked in: e1000e(O) 8139too e100 tsyncpci(O) pps_core
kernel: Pid: 8535, comm: sh Tainted: G O 3.8.13-gentoo #1 /AMD-GX3
```

```

kernel: EIP: 0060:[<00000028>] EFLAGS: 00010202 CPU: 0
kernel: EIP is at 0x28
kernel: EAX: d4d684d0 EBX: dbfaffb4 ECX: ded98820 EDX: 58deea96
kernel: ESI: b752f9e0 EDI: c1021e50 EBP: dbfaffa4 ESP: dbfaff34
kernel: DS: 007b ES: 007b FS: 0000 GS: 0033 SS: 0068
kernel: CR0: 8005003b CR2: 00000028 CR3: 1be71000 CR4: 00000090
kernel: DR0: 00000000 DR1: 00000000 DR2: 00000000 DR3: 00000000
kernel: DR6: fff0ff0 DR7: 00000400
kernel: Process sh (pid: 8535, ti=dbfae000 task=deea96c0 task.ti=dbfae000)
kernel: Stack:
kernel: 00000010 dbfaff48 deea96c0 ded98858 dbfaffb4 ded98820 00000028 00000004
kernel: dbfaff80 c109f0b6 00000001 00000000 00000000 d4c3f908 dec0d8d0 de8e8800
kernel: deea9960 deea96c0 00000000 dbfaff88 c109f228 dbfaff9c c10404a6 00000002
kernel: Call Trace:
kernel: [

```

## inode entries

Example entry “RC-GPSNTP01 kernel: ext3\_orphan\_cleanup: deleting unreferenced inode 9967”

## Example from a unit that may have a bad ETX:

**Note:** all of these entries were asserted on the same day at the same second.

```

kernel: ext3_orphan_cleanup: deleting unreferenced inode 99679
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99678
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99677
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99676
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99675
kernel: EXT3-fs (hda1): 5 orphan inodes deleted

```

---

## Segfaults in Kernel log / SNMPd crash

- Segfaults are BAD
- Segfault errors asserted in kernel log-kern.log when SNMPd crashes.
- Refer to the SNMP troubleshooting section in this document.
- Refer to Mantis case 2995.
- Oleg applied a patch to SNMP in update version 5.2.1 to resolve this intermittent crashing.

## Examples of segfaults related to SNMPS and SNMPSAD

```

kernel: snmpsad[3407]: segfault at 37613038 ip b7575cb8 sp bff470f0 error 4 in libnetsnmp.so.25.0.1[b750e000+ae000]
kernel: snmpd[1892]: segfault at 2774388b ip b74c4032 sp bfb4cd60 error 4 in libnetsnmp.so.25.0.1[b7488000+ae000]

```

**Note:** these particular SNMP segfaults were observed in software version prior to 5.2.0. If this type of entry is observed in the kernel log, update to v5.2.1 or higher. 5.2.1 and above applied a patch update to Net-SNMP that is likely to prevent SNMPd from crashing when walking the mibs.

### **SMBus Timeout followed by Failed reset at end of transaction (01)**

- Refer to cases such as 195780 (June 2019) and 232034 (8 May 2020)
- “SMBUS” is apparently the monitoring bus on the ETX module.

**Email from Dave L to Apps Engineering (25 June 2019)** We have a returned Securesync that experienced failures in the field where it locked up and needed power cycle to restore operation.

This was a Securesync sold in November v5.8.2 with new style ETX.

It was returned to us and we have not been able to duplicate the problem.

I see these strange messages in the logs. Do you know what these might be attributed to?

```
May 22 11:04:41 Spectracom kernel: i2c i2c-3: SMBus Timeout!  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: Failed reset at end of transaction (01)  
May 22 11:04:41 Spectracom kernel: clocksource: Switched to clocksource tsc  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: SMBus Timeout!  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: Failed reset at end of transaction (01)  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: SMBus Timeout!  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: Failed reset at end of transaction (01)  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: SMBus Timeout!  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: Failed reset at end of transaction (01)  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: SMBus Timeout!  
May 22 11:04:41 Spectracom kernel: i2c i2c-3: Failed reset at end of transaction (01)
```

Some Securesync have these and some do not. Is this cause to replace the ETX?

---

## mail.log (Mail log entries)

- This system log is not accessible from the browser. But it's in the Save Logs bundle.
- This log is not wiped when performing a "clear all logs" in the browser
- This log is not viewable from the web browser (can FTP it out as a single log, bundle it with all of the logs or view it with telnet/ssh)

---

## manifest.log file /manifest.config file

- New log and config file added in update **version 5.7.1** (not available in versions 5.7.0 and below)

**Note** the manifest log is not listed in the **Tools** drop-down, like other Spectracom logs.

**Description (from Engineering Release Notes)** Added a SecureSync/Netclock 94XX Manifest file in /home/spectracom/config/manifest.conf and a Manifest Log in /home/spectracom/log/manifest.log. The config file contains the current software/fpga/firmware versions, option cards and licenses installed. The Log shows these as they change at each reboot.

### File storage locations:

- manifest.conf file is located in the /home/spectracom/config/ directory
- **manifest.log** file is located in the **/home/spectracom/log/** directory

### Command to display the entire manifest.log in cli interface (v5.7.1 and above only)

Type: **manifest** <enter>

## Example manifest log entry:

```
File Edit Format View Help
#####
Fri Mar 30 19:16:47 UTC 2018
#####
SecureSync
Model No: 1200-233
Serial No: 8716
Power: AC 110/220, DC 24-48V
OSC : Rb
GPS : SPS GNSS Rcvr
TEMP : EXT-TEMP
-----
Software      5.7.1
Timing System 3.4.4
Build Time    Aug 18 2017 19:44:33
-----
Linux Kernel: 4.4.26-gentoo
-----
ETX Board: SOM-4455
-----
XO Oscillator Type: OCXO (5ppb)
-----
GNSS Receiver Mfr/Mdl: Trimble RES-SMT GG
Versions: 1.6 1.9 0 0
-----
Option Card Slot 1: 1204-1F
|->Card ID: 0x1F
|->Card Version: 0x01
|->FPGA ID: 0x1F
|->FPGA Version: 0x0103

Option Card Slot 2: 1204-06
|->Card ID: 0x06
|->Card Version: 0x02
|->FPGA ID: 0x00
|->FPGA Version: 0x0000

Option Card Slot 3: Empty

Option Card Slot 4: 1204-12
|->Card ID: 0x12
|->Card Version: 0x01
|->FPGA ID: 0x12
|->FPGA Version: 0x0105

Option Card Slot 5: 1204-02
|->Card ID: 0x02
|->Card Version: 0x01
|->FPGA ID: 0x02
|->FPGA Version: 0x0116

Option Card Slot 6: 1204-01
|->Card ID: 0x01
|->Card Version: 0x01
|->FPGA ID: 0x01
|->FPGA Version: 0x0103
-----

DCS Get Options (1) available Licenses :

License 0: TIMEKEEPER
-----
Runtime: 2159 days 23 hours 0 minutes (3110340 ticks)
#####
Wed Apr 4 12:56:00 UTC 2018
#####
```

---

## mysql\_create.log (MySQL log entries)

- This is a MySQL log included in the log bundle (not displayed in the browser)
- This log is not accessible from the browser. But it's in the Save Logs bundle.
- This log is not wiped when performing a "clear all logs" in the browser
- This log is not viewable from the web browser (can FTP it out as a single log, bundle it with all of the logs or view it with telnet/ssh).

### "cake" (cakePHP): associated with MySQL entries (CakePHP is used to build web applications)

```
Clear MySQL history
fixing permissions
start mysql-safe in no-write mode so we can administer it no matter what the password is
150210 20:38:23 mysqld_safe Logging to '/var/log/mysql/mysqld.err'.
150210 20:38:24 mysqld_safe Starting mysqld daemon with databases from /srv/mysql
checking if lafayette database exists
result = "lafayette" if its lafayette create db and tables
Shutting down mysql_safe
150210 20:38:25 mysqld_safe mysqld from pid file /var/run/mysqld/mysqld.pid ended
restarting mysql-safe in writing mode
150210 20:38:37 mysqld_safe Logging to '/var/log/mysql/mysqld.err'.
150210 20:38:37 mysqld_safe Starting mysqld daemon with databases from /srv/mysql
Some tables exist
checking if there is mysqlstrings file
Running schema update
```

```
Welcome to CakePHP v2.3.0 Console
```

```
-----
App : app
Path: /srv/www2/app/
-----
```

```
Cake Schema Shell
```

```
-----
Comparing Database to Schema...
```

```
The following statements will run.
```

```
ALTER TABLE `lafayette`.`feature_configs`
  CHANGE `feature_id` `feature_id` varchar(12) NOT NULL,
  CHANGE `local_clock_id` `local_clock_id` int(4) NOT NULL;
ALTER TABLE `lafayette`.`log_sys_mons`
  CHANGE `load01` `load01` float DEFAULT 0 NOT NULL,
  CHANGE `load02` `load02` float DEFAULT 0 NOT NULL,
  CHANGE `load03` `load03` float DEFAULT 0 NOT NULL,
  CHANGE `mem_total` `mem_total` int(11) DEFAULT 0 NOT NULL,
  CHANGE `mem_free` `mem_free` int(11) DEFAULT 0 NOT NULL,
  CHANGE `disk_used` `disk_used` int(11) DEFAULT 0 NOT NULL;
ALTER TABLE `lafayette`.`log_gps_statuses`
  CHANGE `avg_tracked_snr` `avg_tracked_snr` int(11) DEFAULT 0 NOT NULL,
  CHANGE `max_tracked_snr` `max_tracked_snr` int(11) DEFAULT 0 NOT NULL,
  CHANGE `min_tracked_snr` `min_tracked_snr` int(11) DEFAULT 0 NOT NULL;
ALTER TABLE `lafayette`.`notification_emails`
  CHANGE `address` `address` varchar(254) NOT NULL;
ALTER TABLE `lafayette`.`ethernet_logs`
  CHANGE `rx_bytes` `rx_bytes` int(11) DEFAULT 0 NOT NULL,
  CHANGE `tx_bytes` `tx_bytes` int(11) DEFAULT 0 NOT NULL,
  CHANGE `rx_bytes_per_second` `rx_bytes_per_second` int(11) DEFAULT 0 NOT NULL,
  CHANGE `tx_bytes_per_second` `tx_bytes_per_second` int(11) DEFAULT 0 NOT NULL;
ALTER TABLE `lafayette`.`remote_servers`
  CHANGE `host` `host` varchar(255) NOT NULL;
ALTER TABLE `lafayette`.`preferences`
  CHANGE `type` `type` int(4) DEFAULT 0 NOT NULL,
  CHANGE `local_time` `local_time` tinyint(1) DEFAULT '1',
  CHANGE `registration_reminder` `registration_reminder` tinyint(1) DEFAULT '1';
```

```
Are you sure you want to alter the tables? (y/n)
[n] >
Updating Database...
feature_configs updated.
log_sys_mons updated.
log_gps_statuses updated.
notification_emails updated.
ethernet_logs updated.
remote_servers updated.
preferences updated.
End update.
Shutdown mysql_safe
150210 20:38:42 mysqld_safe mysqld from pid file /var/run/mysqld/mysqld.pid ended
```

---

## NTP.log entries (NTP Log entries)

- NTP logs are stored in the NTP System Log. Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/msyslog.html> for a description of several log entries that may be asserted in this log

### Version 4.2.8 logs (software version 5.2.1 and above)

#### A) NTP startup

```
Sep 4 17:07:03 Spectracom ntpd[16050]: ntpd 4.2.8p3@1.3265-o Tue Aug 11 16:01:10 UTC 2015 (1): Starting
Sep 4 17:07:03 Spectracom ntpd[16050]: Command line: /usr/sbin/ntpd -p /var/run/ntpd.pid -g -c /etc/ntp/ntp.conf
Sep 4 17:07:03 Spectracom ntpd[16052]: proto: precision = 3.108 usec (-18)
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen and drop on 0 v6wildcard [::]:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen and drop on 1 v4wildcard 0.0.0.0:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen normally on 2 lo 127.0.0.1:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen normally on 3 eth0 10.2.100.176:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen normally on 4 eth1 10.2.100.27:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen normally on 5 lo [::1]:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen normally on 6 eth0 [fe80::2d0:c9ff:feba:ebc9%5]:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listen normally on 7 eth1 [fe80::20c:ecff:fe05:44e%6]:123
Sep 4 17:07:03 Spectracom ntpd[16052]: Listening on routing socket on fd #24 for interface updates
Sep 4 17:07:03 Spectracom ntpd[16052]: PCI_TSYNC(0) 8011 81 mobilize assoc 24673
Sep 4 17:07:03 Spectracom ntpd[16052]: PPS(0) 8011 81 mobilize assoc 24674
Sep 4 17:07:03 Spectracom ntpd[16052]: 10.2.100.177 8011 81 mobilize assoc 24675
Sep 4 17:07:03 Spectracom ntpd[16052]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Sep 4 17:07:03 Spectracom ntpd[16052]: 0.0.0.0 c012 02 freq_set kernel -79.685 PPM
Sep 4 17:07:03 Spectracom ntpd[16052]: 0.0.0.0 c016 06 restart
Sep 4 17:07:04 Spectracom ntpd[16052]: PCI_TSYNC(0) 8024 84 reachable
Sep 4 17:07:04 Spectracom ntpd[16052]: PCI_TSYNC(0) 903a 8a sys_peer
Sep 4 17:07:04 Spectracom ntpd[16052]: 0.0.0.0 c415 05 clock_sync
Sep 4 17:07:05 Spectracom ntpd[16052]: PPS(0) 8024 84 reachable
Sep 4 17:07:05 Spectracom ntpd[16052]: PPS(0) 903a 8a sys_peer
Sep 4 17:07:06 Spectracom ntpd[16052]: 10.2.100.177 8024 84 reachable
Sep 4 17:07:03 Spectracom ntpd[16050]: ntpd 4.2.8p3@1.3265-o Tue Aug 11 16:01:10 UTC 2015 (1): Starting
Sep 4 17:07:03 Spectracom ntpd[16050]: Command line: /usr/sbin/ntpd -p /var/rSep 4 17:07:30 Spectracom ntpd[16052]: ::1
config: fudge 127.127.22.0 refid GPS
```

---

#### B) NTP statistics logging (Client and server NTP packets per second)

- Added this new NTP logging feature in software update version 5.2.1 (Apr 2015) as part of NTP v4.2.8 upgrade

#### Provides NTP throughput / NTP loading

- Entries are asserted into the NTP.log (NTP Log)
  - **Example log entry (with no clients):** NTP statistics: Clients = 0.000 pkt/s, Servers/Peers = 0.000 pkt/s
  - **Example log entry (with just a couple clients) NTP statistics:** Clients = 0.037 pkt/s, Servers/Peers = 0.000 pkt/s

**Note:** pkt/s is reported in Mbps (Megabits/sec). So 0.140 pkt/s is 1400 packets per second ???

#### Where:

- **Clients:** NTP requests from NTP clients on the network
- **Servers/Peers:** NTP requests from Servers or Peers configured to get time from this SecureSync



## 1. To convert pkt/s (values in the graphs/logs) to the actual number of packets in the hour

**Multiply** the number of pkt/s (value in the graphs/logs) times **60** and then round-up to nearest whole number

Examples:

0.017 pkt/s = 1 packet in one hour  
0.083 pkt/s = 5 packets in one hour  
0.167 pkt/s = 10 packets in one hour  
1.667 pkt/s = 100 packets in one hour  
166.667 pkt/s = 10,000 packets in one hour  
3000 pkt/s = 180,000 packets in one hour

## 2. To convert actual number of packets per hour to pkt/s (values in the graphs/logs)

**Divide** the number of ntp packets in the hour by **60** (there are 60 minutes in the report period)

Examples:

1 packet in one hour = 0.017 pkt/s  
5 packets in one hour = 0.083 pkt/s  
10 packets in one hour = 0.167 pkt/s  
100 packets in one hour = 1.667 pkt/s  
10,000 packets in one hour = 166.667 pkt/s  
180,000 packets in one hour = 3000 pkt/s

---

### C) NTP on-the-fly config changes

::1 config: fudge 127.127.22.0 refid GPS

::1 config: fudge 127.127.22.0 refid PPS

- These entries are only present if the PPS Atom Clock driver is enabled
- Indicate the Atom clock driver is fudging the value of what it's synced with (its synced to GPS, PPS, etc)

10.2.100.177 local addr 10.2.100.176 ->

10.2.100.58 local addr 10.2.100.176 ->

- These entries indicate peers have been added to the ntp.conf file.

---

### D) NTP state change

ntpd 4.2.8p2@1.3265-o Tue Apr 21 15:01:53 UTC 2015 (1): Starting

ntpd exiting on signal 15 (Terminated)

Listen and drop on 1 v4wildcard 0.0.0.0:123

---

### E) KoD (Kiss of Death) packet

- refer to (in this document): [Kiss of Death packets \(KOD\) for SecureSync/9400s](#)

example KoD packet from a customer log bundle (v5.7.1)

Jul 9 07:53:45 amrc11101 ntpd[23494]: receive: Drop 0 origin timestamp from sym\_active@10.115.218.53 xmt

0xdeed930c.842f2072

Jul 9 07:54:12 amrcl1101 ntpd[23494]: receive: KoD packet from 10.115.218.53 has a zero org or rec timestamp. Ignoring.

## F) A Peer/Server unreachable or is toggling back-forth between reachable and unreachable

example of toggling between reachable and unreachable

```
Jul 9 06:32:55 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul 9 06:33:02 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul 9 06:33:59 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul 9 06:34:05 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul 9 06:35:03 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul 9 06:35:09 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul 9 06:36:07 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul 9 06:36:15 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul 9 06:37:12 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul 9 06:37:18 amrcl1101 ntpd[23494]: 10.210.96.25 8014 84 reachable
Jul 9 06:38:16 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul 9 06:38:21 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul 9 06:39:20 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul 9 06:39:24 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul 9 06:40:24 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
```

### Potential solutions/tests to perform

1. make sure all switch ports that SecureSync is connected to are set to auto-negotiate (v5.7.1 and below) or match the hard-coded settings in the SecureSync (5.8.0 and above only).
2. Periodically perform the following CLI commmad via telnet/ssh connection: **tracpath -p 123 xxx.xxx.xxx** (where x is the IP address or hostname of the peer/server which is unreachable. See if the SecureSync is always able to reach the peer or server.

## G) FIPS 140-2 compliancy/issues with Symmetric key authentication/peering issues

### MAC decrypt: MAC length error

- Refer to Salesforce Case 192055
- Customer experiencing issues peering 5.8.2 SecureSync with a Solaris box running NTP (two Solaris boxes peered OK)
- **System log also contained:** [system] ERROR! NTP generic status polling: Ntpq error: 6 NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ\_UTIL\_STATUS) (STATUSD)
- might be related to NTP FIPS Mode as described in this article??  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=1442083](https://bugzilla.redhat.com/show_bug.cgi?id=1442083)

### (STATUSD errors) (such as extended status polling)

#### General response email from Keith (20 Nov 17) for statusd “extended status polling” error messages in the NTP log

For your information and better understanding, “statusd” is a process used to continually obtain NTP status information via NTP’s NTPQ query tool. Examples of this current status info includes NTP’s current NTP Stratum value, offset values, info on its NTP peers, etc. This information obtained from NTP via the NTPQ query is then provided via various SecureSync outputs- such as via SNMP, the SecureSync’s web browser, its front panel LCD (if its configured to display NTP status, etc).

The log entries you observed just indicate that NTPQ was busy when it was queried, so it wasn’t able to respond with NTP’s status at that particular moment. The statusd program continued asking NTPQ for this status data (as it always does, to have the most recent status info available from NTP) and once NTPQ was available again to provide the status data to the rest of the system, it provided it and the log entries indicating that it was previously too busy to respond, stopped being asserted.

In summary: seeing these NTP log entries periodically asserted is not an indication of a problem with the SecureSync or its NTP functionality! They just indicate NTPQ (not NTP) was just too busy at a particular moment to be able to provide NTP status info

### 1) “NTP extended status polling...” combined with “Type mismatch”

- Refer to Salesforce cases 117236 and 121454

```
[system] ERROR! ERROR!!!! NTP extended status polling: Type mismatch. Expected: 3, Actual: 0
/usr/src/spectracom/easycpp/src/EasyCpp/Settings/Variant.cpp, 110, void
Easy::Settings::Variant::CheckThatTypels(Easy::Settings::Variant::enuType) const (STATUSD)
```

#### Likely causes:

- 1) NTPQ was just momentarily busy and couldn't respond

**Email from Paul Myers (20 Nov 19)** I believe we cannot momentarily communicate with NTP successfully. It is an intermittent error condition. It can or errors like it can occur when NTP is restarting. The NTP extended status polling is the error source. I dig down into the actual 3 versus 0 value enum.

```
4 Nov 07 13:22:19 [system] ERROR! ERROR!!!! NTP extended status polling: Type mismatch. Expected: 3, Actual:
0 /usr/src/spectracom/easycpp/src/EasyCpp/Settings/Variant.cpp, 110, void
Easy::Settings::Variant::CheckThatTypels(Easy::Settings::Variant::enuType) const (STATUSD)
```

- 2) Kernel lock-up issues: with at least case 117236, these NTP entries were also accompanied by kernel errors of bug/oops/call trace type entries (with version 5.7.1 software installed)

---

### 2) “extended status polling: Ntpq error” combined with entry [system] System command error: NTPQ\_GetAsscVariable\_Actual (NTPAL)

- Refer to Salesforce cases such as 117690

```
[system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
```

#### (6 Sept 17 KW) Paul M responded w/info and my response to customer below:

Regarding your inquiry pertaining to the two SecureSync log entries, I found out these logs entries are tied to each other and are associated with the process used to obtain status information from NTP (via the “ntpq” query tool). This status info includes items such as NTP’s sync status and current stratum value, info about its NTP peers, etc.

These two log entries are messages asserted when ntpq can't temporarily communicate with NTP to obtain its most current status data. These entries are likely to be seen when NTP had just been just restarted (or NTP hasn't yet started-up after a reboot/power cycle of the SecureSync (NTP isn't fully running yet when ntpq requests the status data).

These two linked entries are not something to be alarmed about. The ntpq query will once again start obtaining the NTP status data that its requesting from NTP once NTP is again able to communicate with ntpq

---

### 3) Popcorn spike ntpd[4639]: 74.123.28.4 942d 8d popcorn 0.000040 s

- Apparently can just be just a logging bug (<https://tools.cisco.com/quickview/bug/CSCug48022>)
- “Popcorn” is part of the Clock Filter algorithm
  - from <http://tools.ietf.org/html/draft-ietf-ntp-ntpv4-algorithms-01>

“A 'popcorn spike' is a transient outlier, usually only a single sample, that is typical of congested Internet paths. The popcorn spike suppressor is designed to detect and remove them. Let  $\theta_{prime}$  be the peer offset determined by the previous message and  $\psi$  the current peer jitter. If  $|\theta - \theta_{prime}| > (K_s * \psi)$ , where  $K_s$  is a tuning parameter that defaults to 3, the sample is a popcorn spike and is discarded.”

### 4) sys\_peer

#### 140.142.16.34 941a 8a sys\_peer (where the numbers at the beginning are an IP address)

- Refer to sites such as: <http://osdir.com/ml/comp.protocols.time.ntp/2011-05/msg00022.html>
- Appears this is an abbreviated entry (starting in NTP v4.2.6 and above) to indicate a new peer has been selected for sync. The stratum value of the peer is no longer reported (like it was in earlier versions of NTP). In the log entry above, NTP is now synced with 140.142.16.34.

#### 5) no\_sys\_peer

- Appears this is an abbreviated entry (started in 4.2.6 and above) to indicate a peer has been lost. Stratum value of the peer is no longer reported. In the log entry below, NTP is no longer synced to any peer

```
ntpd[5186]: 0.0.0.0 c618 08 no_sys_peer
0.0.0.0 c614 04 freq_mo
```

#### 6) Frequency error xxx.xxx.xxx.xxx PPM exceeds tolerance 500 PPM

The max tolerance is set in <ntp-source-tree>/include/ntp\_proto.h by  
#define NTP\_MAXFREQ 500e-6c (Note: customers don't have permissions to edit the limit of 500 PPM)

#### 7) Ipv6 error entries present, even though IPv6 isn't configured

```
20 Jun 15:53:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign
requested address
20 Jun 15:53:17 ntpd[2016]: unable to create socket on eth0 (9) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 15:53:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 15:58:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign
requested address
20 Jun 15:58:17 ntpd[2016]: unable to create socket on eth0 (10) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 15:58:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 16:03:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign
requested address
20 Jun 16:03:17 ntpd[2016]: unable to create socket on eth0 (11) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 16:03:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 16:08:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign
requested address
20 Jun 16:08:17 ntpd[2016]: unable to create socket on eth0 (12) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 16:08:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 16:13:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign
requested address
20 Jun 16:13:17 ntpd[2016]: unable to create socket on eth0 (13) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 16:13:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
```

- Appears to be associated with the Ethernet port (eth0) supporting both IPv4 and IPv6, and NTP is not being forced to using only IPv4.
- Refer to sites such as <http://www.linuxquestions.org/questions/linux-server-73/getting-ipv6-errors-in-ntp-4175525840/> and <https://bugs.launchpad.net/ubuntu/+source/ntp/+bug/700492>

#### 8) Unexpected origin timestamp xxxxx.xxxxx does not match aorg 00000.00000 from xx

##### Example entries

```
Jul 12 15:04:28 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227
xmt 0xdb2f857c.349efd85
Jul 12 15:22:34 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227
xmt 0xdb2f89ba.349ec968
Jul 12 15:40:11 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227
xmt 0xdb2f8ddb.34a0dfa1
```

#### Summary of the info further below

##### A) (Versions 5.4.4 and below)

- Actual NTP operation issue with loss of peer response prior to NTPv4.2.8p7

## B) (Versions 5.4.5 to at least 5.8.4, and likely even higher)

- Errant NTP logging issue only – not an indication of operational NTP issue (these log entries are carryover from the issue in earlier NTP versions, and can simply be ignored/disregarded)
- Refer to Salesforce Cases such as 185388
- This is a bug in NTP- Reportedly fixed in NTP v4.2.8p7 (SecureSync versions 5.4.4 and below are susceptible. We are expecting to update to 4.2.8p7 in v5.4.5) For more info on this NTP bug, refer to: [http://bugs.ntp.org/show\\_bug.cgi?id=2952](http://bugs.ntp.org/show_bug.cgi?id=2952)
- in earlier NTP versions it appears to cause intermittent loss of communications (NTP timestamps between peers), intermittent loss of time stamps from a peer and so the Peer(s) Reach value goes to 0.
- Refer to sites such as: <https://www.suse.com/support/kb/doc?id=7017645> (except pasted below)

### Situation

Having peer servers configured as part of the NTP configuration, the following messages are logged in "/var/log/ntp":

ntpd[xxxx] receive: Unexpected origin timestamp xxxxx.xxxxx does not match aorg 00000.00000 from xx (Where xx at the end of the message is the IP address of the configured peer server). Eventually this results in communication failure between the configured servers.

### Resolution

Update NTP to version 4.2.8p7 or above (SecureSync versions 5.4.4 and below are susceptible. We are expecting to update to 4.2.8p8 in v5.4.5)

### Cause

This was caused by changes made to bogus packet detection of NTP. Although the messages are still logged with the current latest NTP version, communication is not lost anymore and the messages can be ignored.

Example email Keith sent to customer (18 Feb 2019) Regarding Orolia/Spectracom Case Number 185388, I had mentioned that it appeared from the SecureSync's NTP log entry "**unexpected origin timestamp**" that there was apparently an issue with the NTP data it was getting from its NTP peer (the NIST time server)

Sorry about the delay in being able to get back to you with more info about this (As I like to say, there are just never enough hours in the day, days in the week or weeks in the year 😊)!!!

I worked with one of our Apps engineers about the log entry I had noticed in the log bundle. He found details online that this entry was a factor of NTP peering and the entry can be simply disregarded. It's not an indication the peer is providing invalid time (though it's easy to think this, based on the wording of the entry).

I configured one of our time servers to peer with this same time server, and I am seeing the exact same log entry present in our NTP logs, as well.

Per websites such as: <https://www.suse.com/support/kb/doc/?id=7017645> (Excerpt below)

### Situation

Having peer servers configured as part of the NTP configuration, the following messages are logged in "/var/log/ntp":

ntpd[xxxx] receive: Unexpected origin timestamp xxxxx.xxxxx does not match aorg 00000.00000 from xx

Where xx at the end of the message is the IP address of the configured peer server, eventually this results in communication failure between the configured servers.

## Cause

This was caused by changes made to bogus packet detection of NTP. **Although the messages are still logged with the current latest NTP version, communication is not lost anymore and the messages can be ignored.**

Apparently, the “unexpected origin timestamp” log entries sent in earlier versions of NTP (before just being a log entry) used to related to an issue with no timestamps being received from the specified peer.

To see that the version of NTP installed is not losing all packets from the NIST time server (and therefore these log entries can be ignored), just open a CLI connection (telnet/ssh) to the time server. At the command prompt, type: `ntpq -p<enter>`.

The response to this command lists each time reference NTP can sync with (such as the NIST time sever, for example). There is a “reach” value for each listed reference.

The only time the “Reach” value for each reference should normally be “0” is after NTP has just been restarted or the time server just rebooted. Soon after every time NTP has been restarted in either scenario, it should increment (it’s an octal counter, so it will go from 0 to 7, to 17, etc) for each NTP time stamp its receiving from that reference. Reach of 377 indicates that of the last eight requested time requests NTP sent to this reference, it received all eight expected responses.

As long as the Reach for the NIST server isn’t “0”, this NTP log entry can simply be ignored, because nTP in the SecureSync is receiving responses back from the NIST server 😊!

Note there are other factors besides just the version of NTP which can also cause the Reach to be “0” for a peer, such as NTP port 123 being closed on a firewall between the SecureSync and its configured NTP peer. If port 123 is closed, no packets will be received, so reach will remain at “0”.

In summary of the above, there is no need to be concerned there is an issue with the NTP data its receiving from its NTP peer. The LOG entry is part of expected operation when peering with other servers.

---

### NTP Version 4.2.6 and 4.2.0 logs (software versions 5.2.0 and below)

#### clock PCI\_TSYNC(0) event 'clk\_fault' (0x03):

- NTP is no longer synced to the System Time (GPS, IRIG, Stanag, NTP, etc).

#### Deleting interface #3 eth0, 10.2.100.89#123, interface stats: received=0, sent=7, dropped=0, active\_time=103 secs

- This log entry indicates a recent power cycle is resetting/restarting the Ethernet ports (note the values after “Deleting interface” will inherently vary)

---

#### 127.127.1.0 interface 127.0.0.1 -> (none)

- This entry is applicable to versions 5.0.0 and above (not applicable in versions 4.8.9 and below)
- This entry is associated with the Local clock reference no longer being used to go to Stratum 16 (like it previously was in versions 4.8.9 and below).
- When we went to NTP version 4.2.6 in 5.0.0 and above, we changed how we force NTP to go to Stratum 16. Now, the local clock reference is not used.

---

#### Synchronized to PPS(0), stratum=0:

- The Atom clock (PPS) driver provides NTP with a 1pps input that it can discipline with, after NTP has synced to a time reference (such as GPS, for instance). Several minutes after NTP has synced, this NTP log entry will be asserted.

**frequency error xxx PPM exceeds tolerance** (the xxx value will vary):

- a very large time jump of NTP's selected input reference has occurred. The System Time may have been manually changed, while NTP was syncing to it, for example.

---

**kernel time sync disabled 0041:**

- From link above: "The kernel reports an error."
- ntpd doesn't sync kernel time anymore.

**kernel time sync enabled 0001:**

- ntpd is back to syncing kernel time.

---

**no servers reachable:**

- Local Clock reference has been **DISABLED** (in the *Network* -> *NTP Setup* page of the browser, **NTP Servers** tab) and NTP has NO input references to select for its sync. NTP will **NOT** be able to go to Stratum 16, even with no inputs present. NTP clients won't ignore the NTP time stamps (time stamps won't report Stratum 0).

---

**ntpd exiting on signal 15:**

- NTP was disabled in the web browser by a user.
- NTP was automatically restarted after configuration change made to NTP (software versions 5.0.0 and above).
- NTP was restarted by the watchdog (ntpmond) because of a large time change.
- Also appears this entry is asserted upon a reboot of the time server.

---

**[system] KTS Host Time Daemon has restarted**

**Indicates KHTD was restarted**

- **Note:** KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running

---

**pps sync disabled:**

- The Atom clock driver's 1PPS input has died (no longer present in NTP).

---

**peers refreshed:**

---

**synchronized to PCI\_TSYNC(0), stratum=0:**

- NTP synced to the System Time (GPS, IRIG, Stanag, NTP, etc). NTP is reporting its Stratum 1.

**Note:** If this NTP log entry is never being asserted, System Time may never be synced. Also, make sure the "**Timing System Reference**" field is "Enabled" in the *Network*-> *NTP setup* page, "**NTP Servers**" tab, when system Time is an input to NTP (typically, it should only be "Disabled" if NTP is only syncing to other NTP servers and there is no desire to allow NTP to have any holdover capability). If this field is disabled, NTP won't have System Time listed in the Status-> NTP page as an available reference that it can sync with.

Indicates NTP in the SecureSync synced to "System Time" (which is synced to manually set time, GPS, IRIG input ,

have quick input etc – but not NTP). This entry indicates NTP in the SecureSync is now Stratum 1. This entry indicates NTP is not currently synced to another NTP time server. It also indicates NTP clients getting NTP time from the SecureSync won't reject the timestamps (as NTP clients often do, when SecureSync is at Stratum 16).

---

#### synchronized to LOCAL(0), stratum=15:

- NTP has selected the local clock reference, either because no other input is available, or NTP has decided the local reference is better than a single other input reference. NTP is Stratum 16 (NTP time stamps report **Stratum 0**)

**Note:** This entry is applicable only to software versions 4.8.9 and below (NTPv4.2.0)

Indicates NTP in the SecureSync is no longer synced to “System Time” (manually set time, GPS, IRIG input, have quick input etc) and is not synced to any other NTP servers either. This entry means SecureSync is reporting to NTP clients that NTP is now “Stratum 16”, resulting in NTP clients rejecting the NTP time stamps they are receiving from this SecureSync.

#### Notes about this “Local(0)” log entry:

- 1) If there are alternating NTP log entries of “**synchronized to Local(0) ...**” and “**synchronized to PCI\_TSync(0)...**” Make sure the “**Preferred**” checkbox is enabled in the **Network-> NTP setup** page, “**NTP Servers**” tab, when System Time (GPS, user set time, Stanag, etc) is an available input to NTP (typically, it should only be unchecked if NTP is only syncing to other NTP servers and there is no desire to allow NTP to have any holdover capability). This is rare.
- 2) If there are “**synchronized to Local(0)...**” log entries with no “**synchronized to PCI\_TSync(0)...**” log entries, make sure the “**Timing System Reference**” field is “**Enabled**” in the **Network-> NTP setup** page, “**NTP Servers**” tab, when system Time is an input to NTP (typically, it should only be “**Disabled**” if NTP is only syncing to other NTP servers and there is no desire to allow NTP to have any holdover capability). This is rare.

---

time correction of 304925641 seconds exceeds sanity limit (1000); set clock manually to the correct UTC time: (note the number of seconds in the entry will vary):

- The System Time's date/time was changed by this amount of seconds, while NTP was selected to sync to the System Time. This log entry is likely due to a user manually changing the year, date or time while NTP is syncing to System Time.

**Note:** Review the Journal log to see if there are any corresponding “**Set Time for User Reference 0 in slot 0**” entries, which indicate a user had manually changed System Time (this journal entry also indicates if System Time was changed via the browser or by the front panel keypad).



---

## system.log entries

### Model and Serial Number recorded in System Log

- Version 5.2.1 update (Apr 2015) added Model and Serial Number to the System Log at each start-up.

### Option Card wishbone bus (FPGA) communications issue (Fixed in 5.8.8. Applicable to versions 5.8.7 and below) results in “communication error” messages

- Symptoms of peculiar communication error messages in logs (such as these from Salesforce Case 215921)
  - A) "Failed to get license data (DT\_GetPII2Alarm ->KW\_DCS\_GetOptions) (KAD)"
  - B) "Failed to read alarm info from KTS (KAD)"
  - C) "All inputs Detected" / "Power or Configuration Fault"
- Slot Number associated (slots 4, 5 and 6 affected. Slots 1, 2 and 3 are fine).
- Fixed in version 5.8.8 (March 2020)
  - Refer to Upgrade Version 5.8.8 (in Arena) [https://app.bom.com/changes/detail-attach?change\\_id=2400115001](https://app.bom.com/changes/detail-attach?change_id=2400115001)

### Per the version 5.8.8 Release Notes

Updated the FPGA versions of the following option cards to increase communication reliability: 1204-01, 1204-02, 1204-03, 1204-04, 1204-05, 1204-15, 1204-1F, and 1204-23.

---

## \*\*Troubleshooting “Out of memory / Killed process” entries in System Log

### Specific conditions resulting in Out of memory / Killed process” entries

#### 1. Memory leak issue with TACACS operation (associated with at least v5.8.4/5.8.5)

(seen with version 5.8.4 / 2<sup>nd</sup> gen ETX module installed and 5.8.5)

- Example entry “Apr 27 05:03:55 atl1r033-ntp03 kernel: syslogd: page allocation stalls for 14471ms, order:0, mode:0x1c200ca(GFP\_HIGHUSER\_MOVABLE|\_\_GFP\_WRITE), nodemask=(null)”
- Refer to **JIRA Ticket SSS-640**
- Refer to **Case 193787** (seen with v5.8.4/2<sup>nd</sup> gen ETX installed)
- Associated with “memory leak” with 2<sup>nd</sup> gen ETX, version 5.8.4 and TACACS

**Email from Ryan Johnson to Scott Z** I discussed this with Stuart, and not to downplay the issue at all but this particular case looks to be easier to point to a cause than the other mystery kernel crashes that we've seen before. This lockup is actually more similar to the recent VelaSync issue where a particular software process (in this case TACACS) is leaking memory to the point where eventually it's all used up.

It may not be a simple fix however as TACACS is a fairly complex mechanism. Stuart did request additional information on how the customer is using it to hopefully help us be able to recreate the issue. Any use-case like information that you can extract from the customer would be helpful.

**Per Ryan Johnson (6 May 2019)** This is a new issue – we were unaware of it as well. At this point I can't commit to a timeline for resolution other than it almost certainly will *not* be in the next release (5.8.5) as the scope for that is small and already frozen. We still need more information on the cause before understanding how we would potentially fix.

---

#### 2. Many simultaneous NTPQ requests (prior to statusd being added in v5.3.0 and above)

kernel: Out of memory: Kill process 5311 (mysqld) score 149 or sacrifice child  
Aug 17 19:43:40 CSSknMUSalpb01 kernel: Killed process 5311 (mysqld) total-vm:105060kB, anon-rss:72416kB, file-rss:2900kB

Aug 9 23:31:58 CSSknEUKlinhb02 kernel: Out of memory: Kill process 3309 (mysqld) score 148 or sacrifice child  
Aug 9 23:31:58 CSSknEUKlinhb02 kernel: Killed process 3309 (mysqld) total-vm:104840kB, anon-rss:72076kB, file-rss:2996kB

#### Notes:

- Per Oleg: This issue is not likely to cause the browser/ssh to stop responding- just loss of NTP status info.
- Typically associated with lots of open NTPQ requests in versions 5.2.1 and below.
- The specific text in the log entries will vary, depending on specific conditions of this event. Two different sets below)
- The condition associated with these entries can cause loss of web browser and ssh until power cycle, as the ones below resulted in (refer to Salesforce case 18972 for details).
- Upgrade version 5.3.0 (Sept 2015) is expected to fix this condition (this note is prior to 5.3.0 being fielded, so “time will tell” if this condition is prevented in this new version).
- The new daemon added in version 5.3.0 that is controlling the NTPQ requests was initially called masterd but was renamed shortly thereafter as statusd

#### Steps to diagnose/fix

- 1) Recommend software update to at least version 5.3.0
- 2) If still occurs in 5.3.0 (or above): Per Ron Dries earlier recommendations, get both the unit's logs and config files. Review the System log to find out what the Out Of Memory Manager was trying to kill when the log entry was asserted.

---

#### Management -> Notifications page of the browser associated System log entries

- In at least version 5.4.1, submitting any changes in the Management -> Notifications page of the browser will result in the following group of log entries being asserted in the System log (daemons are restarted when changes are submitted)

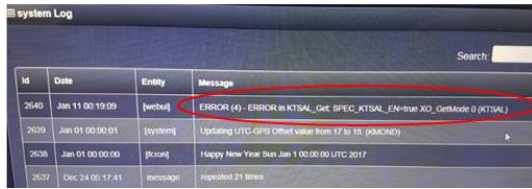
```
Apr 4 21:43:22 CustService176 CustService176: [system] Notification daemon has restarted (NOTD)
Apr 4 21:43:22 CustService176 CustService176: [system] Enabling alarm mask for event: 53 (NOTD)
Apr 4 21:43:22 CustService176 CustService176: [system] Enabling alarm mask for event: 2 (NOTD)
Apr 4 21:43:22 CustService176 CustService176: [system] Enabling alarm mask for event: 55 (NOTD)
Apr 4 21:43:22 CustService176 CustService176: [system] GPS Monitor daemon has restarted (GPSD)
Apr 4 21:43:22 CustService176 CustService176: [system] Received reset request (STATUSD)
Apr 4 21:43:22 CustService176 CustService176: [system] NTP generic status polling (pid=3333, tid=b5cffb40): thread started (STATUSD)
Apr 4 21:43:22 CustService176 CustService176: [system] NTP extended status polling (pid=3333, tid=b7012b40): thread started (STATUSD)
Apr 4 21:43:22 CustService176 CustService176: [system] Temperature Monitoring (pid=3333, tid=b66ffb40): thread started (STATUSD)
```

---

#### KTSAL Timing system related entries

ERROR (4) – ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true XO\_GetMode 0 (KTSAL)  
ERROR (4) – ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true SS\_GetTfom 0 (KTSAL)

Q I have a question about system log of SecureSync.



The screenshot shows a 'system Log' window with a search bar and a table of log entries. The table has columns for 'id', 'Date', 'Entity', and 'Message'. The entry with id 2640 is circled in red. The message for this entry is 'ERROR (4) - ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true XO\_GetMode 0 (KTSAL)'.

| id   | Date            | Entity    | Message                                                                 |
|------|-----------------|-----------|-------------------------------------------------------------------------|
| 2640 | Jan 11 00:19:09 | [webui]   | ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetMode 0 (KTSAL) |
| 2639 | Jan 01 00:00:01 | [system]  | Updating UTC-GPS Offset value from 17 to 18. (WOMOND)                   |
| 2638 | Jan 01 00:00:00 | [cron]    | Happy New Year Sun Jan 1 00:00:00 UTC 2017                              |
| 2637 | Dec 28 00:17:41 | [message] | Received 21 bytes                                                       |

**A Reply from Dave L (13 Jan 17)** These types of error messages can appear in the System Log from time to time. This particular error has been reported because a process to read the oscillator mode was interrupted for some reason.

We believe they are caused by web UI pages terminating, or unexpected signals. There is no cause for alarm. Similar messages may appear in all Securesyncs.

### NTPQ/statusd (Status daemon) associated System log entries

- I believe statusd daemon was originally implemented by Oleg. But Timofey modified it for at least version 5.4.1 (I believe Ron Dries said Timofey also modified it for version 5.3.1 but not positive on this).
- statusd obtains NTP status info via NTPQ data and stores it in a temporary location for various threads to access this info.

### System command error fpanel:DT\_DrawStat (FPD)

Example entry: [system] System command error fpanel:DT\_DrawStat (FPD)

#### A) Versions 5.4.1 and above

**Modified email from Paul Myers (22 Aug 16) regarding a unit with many of these entries** These entries indicate front panel is locked up. They are likely running in a degraded state. Could the TSYNC Driver be unloaded? Is the FPGA failure being reported in the system log?

#### B) Version 5.3.0 and below

This status information reported on the front panel (if the SecureSync has been configured to display Status information instead of the network settings, as many customers choose to display) includes the NTP Stratum and NTP Sync status. Software update version 5.3.0 incorporated changes in how info from NTP is obtained for items such as the web browser, SNMP, the CLI interface and the front panel to report (v5.3.0 added statusd daemon to have one location for threads to get NT status info)

**Note from Keith:** I've seen this error entry in version 5.3.0, as well. Suspect it's due to an OCXO oscillator glitching/starting to fail.

- Per Oleg- This issue is not likely to cause the browser/ssh to stop responding- just loss of NTP status info.
- This daemon was initially called 'masterd';

Changes made in **Management** -> **Notifications** page of browser results in ERROR message asserted in system.log

**ERROR! Caught signal 6 (Aborted)**, address=000000000000b34, pid=2868 (not reliable), tid=b7653580 (not reliable)  
Backtrace: /lib/libEasyCpp.so(\_ZN4Easy11crashActionEiPvS0\_+0x1af) [0xb7b8075f]  
/lib/libEasyCpp.so(\_ZNK4Easy8FunctionlvNS\_8TypeListIiPvS2\_NS\_9EmptyTypeES3\_EEPFviS2\_S2\_EEcIeiS2\_S2\_+0x24) [0xb7b82a68] /lib/libEasyCpp.so(\_ZNK4Easy6ActionlvNS\_8TypeList

### Associated Journal log entry (asserted same date/time) [WEB] Enabling minor alarm when less than 3 sats for 3 seconds (spadmin)

- Per Ron Dries, this Signal 6 entry can be asserted when any changes are made in the *Management* -> *Notifications* page of the browser. When changes are made to **Notifications** (such as masking alarms, changing temperature alerts, etc) the statusd daemon automatically restarts in the background, resulting in a "signal 6" entry.
- Verify the Journal log has a correlating entry for changes being made to Notification configuration being changed, then this entry was asserted in the System log.

---

## Temperature Monitoring

### Two related error messages: **Error 4** and **Error 5** (both associated with Temperature Monitoring)

- Both of these messages are due to a Minor Issue found in v5.7.0? and fixed in 5.7.1
  - Refer to JIRA case **SSS-293** for both entries
  - **Note:** SF case 171143 reported it was already at 5.7.1 when this entry was asserted (it was supposed to be fixed in 5.7.1). He is going to update to 5.8.1 and see if it occurs again.
  -

#### C) "Error 4" message

[system] ERROR! ERROR!!!! Temperature Monitoring: Failed to read CPU temperature. Error: 4 /usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double Hw::Cpu::Temperature() (STATUSD)

- Refer to SF case 118395

**Email from Ryan (28 Sept 17)** This error isn't a concern. There was a bug where sometimes we'd attempt to read the temperature at the same time when it was being updated, resulting in a conflict and the error. The next time it would try and likely succeed so it would be just an occasional conflict.

This is fixed in 5.7.1: <https://spectracom.atlassian.net/browse/SSS-293?dest-url=/plugins/servlet/mobile>

#### D) "Error 5" message

Aug 10 15:07:53 <local7.emerg> ptp201 ptp201: [system] ERROR! ERROR!!!! Temperature Monitoring: Failed to read CPU temperature. Error: 5 /usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double Hw::Cpu::Temperature() (STATUSD)

- Refer to SF cases 171143, 116678

**Customer Report:** I've powered-up and reconfigured the repaired Securesync server, including sending all the logging to my syslog server. It's been sending some messages that are concerning:

```
Aug 10 15:07:53 <local7.emerg> ptp201 ptp201: [system] ERROR! ERROR!!!! Temperature
Monitoring: Failed to read CPU temperature. Error: 5
/usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double
Hw::Cpu::Temperature() (STATUSD)
Aug 10 15:07:53 <local7.emerg> ptp201 ptp201: [system] ERROR! ERROR!!!! Temperature
Monitoring: Failed to read CPU temperature. Error: 5
/usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double
Hw::Cpu::Temperature() (STATUSD)
```

By this time the unit had been running for a few hours.

- A Reply from Dave L (14 Aug 17)** There messages are from the System log and I think they indicate the CPU Temperature data is not being logged correctly. I am verifying with engineering. When was this repaired? Do you have a RMA number or serial number we can record?
- A email from Ryan (14 Jul 17)** This is addressed in 5.7.1 (SSS-293 in Jira) and I'll update the SF ticket. The problem itself is innocuous and is a symptom of occasionally being unable to read the temperature. These are Stuarts comments:

I have verified that there are periods of time that the kernel takes down the temperature input file that is being read (/sys/class/hwmon/hwmon0/temp\_input2).

Very rarely, statusd will attempt to read this file at the exact same time the kernel takes it down - so the easiest way to prevent this is (as paul suggested) implement a retry capability so it will try a few times after a small delay.

**A Second reply from Dave L (14 Aug 17)** The problem is a symptom of occasionally being unable to read the temperature. We have a ticket in to create the resolution. Thank you and your customer for your patience while we resolve this issue.

---

## NTP/statusd associated System log entries

“System command error: NTPQ\_” / “NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ\_UTIL\_STATUS) (STATUSD)”

➤ Refer to SF case 119824 / JIRA ticket JIRA-SSS-202

- JIRA ticket was written for version 5.5.0, but is still unresolved in at least version 5.7.1

```
Sep 30 11:13:27 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Sep 30 11:13:27 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
```

```
Sep 30 11:14:09 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Sep 30 11:14:09 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
```

```
Oct 7 12:03:57 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 7 12:03:57 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
```

```
Oct 7 12:05:21 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 7 12:05:21 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
```

```
Oct 13 08:26:26 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:26:26 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
```

```

/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:28:00 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:28:00 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:29:34 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:29:34 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:31:07 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:31:07 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:31:49 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:31:49 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/s

```

**Per Paul Myers (13 Oct 17) JIRA-SSS-202** records this issue in Release 5.5.0 and is assigned to Ryan for disposition. This issue appears to be an intermittent polling failure to communicate between StatusD and NTPD using ntpq. We have not directly addressed or investigated it. I believe it is just a failure of status to communicate with NTPD. However, 5.7.1 has made improvement to NTPD (new version) and has corrected issues with StatusD operation and restart. Based on Security vulnerabilities and these improvements it is recommended to update.

---

**Statusd keeps resetting (isn't able to start) because the Min CPU temperature threshold values have been reconfigured by a user to be greater than "100" (100 is the max value)**

- In at least version 5.4.1, the web browser doesn't restrict/alert to setting the thresholds to above 100 (the max value that the system allows these values to be).
- The following log entry ("statusd has started") is continuously asserted because statusd keeps resetting.
- NTP Status (Stratum, Sync state, etc) is reported as "???" because the data obtained with NTPQ keeps being deleted.

```

Apr  4 22:02:23 CustService176 CustService176: [system] statusd has started (STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP generic status polling (pid=14524, tid=b6fa7b40): thread started
(STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP extended status polling (pid=14524, tid=b65ffb40): thread started
(STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] statusd has started (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP generic status polling (pid=16331, tid=b6f37b40): thread started
(STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP extended status polling (pid=16331, tid=b65ffb40): thread started
(STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] statusd has started (STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] NTP generic status polling (pid=18199, tid=b6f45b40): thread started
(STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] NTP extended status polling (pid=18199, tid=b65ffb40): thread started
(STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] statusd has started (STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP generic status polling (pid=14524, tid=b6fa7b40): thread started
(STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP extended status polling (pid=14524, tid=b65ffb40): thread started
(STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] statusd has started (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP generic status polling (pid=16331, tid=b6f37b40): thread started
(STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP extended status polling (pid=16331, tid=b65ffb40): thread started
(STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] statusd has started (STATUSD)

```

- Refer to the “statusd” section of this document for more info: [Statusd daemon for obtaining status info from NTP \(v5.3.0 and above\)](#) (scroll down to “Issues associated with statusd”)
  - Setting the “**Minimum CPU temperature**” thresholds above “**100**” in at least versions 5.4.0/5.4.1 will cause statusd to continuously reset (this entry will continue to be asserted). Lower the two “Minimum mperaure” values (**Management** -> **Notifictions** page, **System** tab) to “100” or less to keep statusd from resetting and therefore to keep this alarm entry from being consistently asserted.

## 9) System command error” NTPQ\_util\_status (Statusd)

|     |                    |          |                                                                                                                                                                                   |
|-----|--------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 551 | Sep 02<br>12:01:45 | [system] | ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d /usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS) (STATUSD) |
| 550 | Sep 02<br>12:01:45 | [system] | System command error: NTPQ_GetAsscVariable_Actual (NTPAL)                                                                                                                         |

“System command error: NTPQ\_GetAsscVariable\_Actual (NTPAL)” In combination with the followinlog entry:

```
ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, vERROR! ERROR!!!! NTP extended status polling: Ntpq
error: %d /usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void
Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS) (STATUSD)oid Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS) (STATUSD)
```

**Email from Paul Myers (5 Sept 17)** These are the “StatusD” status daemon monitoring NTP. These are errors thrown when it cannot communicate with NTP briefly typically using ntpq to monitor it’s status.

It is often occurring if NTPD is restarted or not yet running. It most often can occur on startup if NTPD steps the system time. This is not something to be alarmed about if it occurs. It might only occur frequently if NTP were NOT responding.

## 10) “ERROR! Caught signal 6 (Aborted)...” in System log

- Refer to Salesforce Case 215921

```
“ERROR! Caught signal 6 (Aborted), address=000000000002162, pid=8546 (not reliable), tid=b7668580 (not
reliable) Backtrace: /lib/libEasyCpp.so(_ZN4Easy11crashActionEiPvS0_+0x1af) [0xb7b9575f]
/lib/libEasyCpp.so(_ZNK4Easy8FunctionlvNS_8TypeListIiPvS2_NS_9EmptyTypeES3_EEPFviS2_S2_EEclEiS2_S2
_+0x24) [0xb7b97a68]
/lib/libEasyCpp.so(_ZNK4Easy6ActionlvNS_8TypeListIiPvS2_NS_9EmptyTypeES3_EEEclEiS2_S2_+0x38)
[0xb7ba8ac8] /lib/libEasyCpp.so(_ZN4Easy19signalActionWrapperEiP9siginfo_tPv+0x92) [0xb7ba7fc0]
/lib/libc.so.6(+0x2d110) [0xb76d3110] /lib/ld-linux.so.2(+0x9a2) [0xb7fca9a2] /lib/libc.so.6(gsignal+0xca)
[0xb76d306a] /lib/libc.so.6(abort+0x182) [0xb76d4c02] /lib/libc.so.6(+0x6da7c) [0xb7713a7c] /lib/libc.so.6(+0x758f4)
[0xb771b8f4] /lib/libc.so.6(+0x76bff) [0xb771cbff] /usr/lib/gcc/i686-pc-linux-gnu/7.3.0/libstdc++.so.6(_ZdlPv+0x18)
[0xb7976f18] statusd(_ZN4Easy13checkedDeleteIN3Ntp7MonitorEEEvPT_+0x2e) [0x4db489]
statusd(_ZN5boost6detail18sp_counted_impl_pdIPN3Ntp7Monit”
```

**Cause: ??**

## 11) “Failed to get license data (DT\_GetPII2Alarm->KW\_DCS\_GetOptions) (KAD)” in System log

- Refer to Salesforce Case 215921

**Cause: ??**

---

## 12) “403 error message” in System log

- Refer to Mantis case 3264

```
[system] ERROR! ERROR!!!! NTP generic status polling:  
AccessError /usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 38, static Ntp::GenericStatus  
Ntp::Instance::ReadGenericStatus() (STATUSD)  
84 Mar 23 18:36:21 [system] ntp monitor restarting ntpd (NTPMOND)
```

**Note from Paul Myers:** NTPD shuts down and restarts when stepping time. The statusd daemon should detect this and reestablish communication - not throw a low level error.

---

## 13) Cannot open /tmp/ntpq.data in NTPQ\_ReadStatus (NTPAL)

- Refer to Salesforce case 20824

**Email from Ole (2 Feb 16 KW):** “I believe the statusd fails because of the error:

```
Jan 22 14:53:14 chl-securesync01 chl-securesync01: [webui] Error (7) on eth0 FAILURE detected in opening temp lease file..  
(SYSAL)”. It cannot get data from NTP if ethernet port is not working.
```

---

## 14) “Ntp monitor restarting ntpd (ntpmond)”

```
[system] ntp monitor restarting ntpd (NTPMOND):  
[system] ntp monitor stopping ntpd, found 3578 second difference followed by  
[system] ntp monitor restarting ntpd (NTPMOND)
```

- NTPMOND “wakes-up” and check NTP every 16 seconds to check if NTP is running and if it's within 1 second of the System Time (while synced to System Time).
- NTPMOND will restart NTP if NTP is in sync and the time error from KTS is 1 second or greater, or if NTP exceeded sanity limit of 1000 seconds (16min 40 sec) which can cause it to stop running

**Note: Per Ron Dries,** NTPMOND “wakes-up” every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resync and be useable again.

**Note:** NTP also has its own Reference time change limits, as well (**NTP step threshold of 128ms**)

- If NTP’s selected input changes by **128 millisecond or less**, NTP **slews** to the reference (maximum rate of 500 microseconds per second)

### Fastest time to slew

- **500us** = 1 second
- **1ms** = 2 seconds
- **64ms** = 128 seconds (2.1 minutes)
- **128ms** = 256 seconds (4.2 minutes)
- 
- If NTP’s selected input changes by **more than 128 milliseconds**. NTP **steps** to the reference

---

## 15) Network DNS issues affect NTPQ’s ability to run

```
Jun 10 20:12:40 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)  
Jun 10 20:12:46 Spectracom Spectracom: [system] System command error: NTPQ_GetAsscVariable (NTPAL)
```



Jun 10 20:12:46 Spectracom Spectracom: [system] NTPQ\_GetAsscVariable(ASSC\_VAR\_OFFSET) returned [rc = 1] (KHTD)  
Jun 10 20:13:19 Spectracom Spectracom: [system] System command error: NTPQ\_RetrievePeersData (NTPAL)  
Jun 10 20:13:26 Spectracom Spectracom: [system] System command error: NTPQ\_ReadSysstats (NTPAL)  
Jun 10 20:13:26 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)  
Jun 10 20:13:49 Spectracom Spectracom: [system] System command error: NTPQ\_RetrieveAsscData (NTPAL)  
Jun 10 20:14:13 Spectracom Spectracom: [system] System command error: NTPQ\_ReadSysstats (NTPAL)  
Jun 10 20:14:13 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)  
Jun 10 20:14:19 Spectracom Spectracom: [system] System command error: NTPQ\_GetAsscVariable (NTPAL)  
Jun 10 20:14:19 Spectracom Spectracom: [system] NTPQ\_GetAsscVariable(ASSC\_VAR\_LEAP) returned [rc = 1] (KHTD)  
Jun 10 20:14:49 Spectracom Spectracom: [system] System command error khtd:DT\_FindNonLocalCandidate (KHTD)  
Jun 10 20:14:59 Spectracom Spectracom: [system] System command error: NTPQ\_ReadSysstats (NTPAL)  
Jun 10 20:14:59 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)  
Jun 10 20:15:19 Spectracom Spectracom: [system] System command error: NTPQ\_GetAsscVariable (NTPAL)  
Jun 10 20:15:19 Spectracom Spectracom: [system] NTPQ\_GetAsscVariable(ASSC\_VAR\_OFFSET) returned [rc = 1] (KHTD)  
Jun 10 20:15:46 Spectracom Spectracom: [system] System command error: NTPQ\_ReadSysstats (NTPAL) when the Timing System and Linux kernel time differ by more than 1 sec

- Update software to at least version 5.3.0 to add “statusd” daemon (adds a central location for threads to be able to get NTP Status info from one location without having to run NTPQ)
- Refer to Salesforce case 18447
- Issues with DNS can prevent NTPQ from being able to run. It needs to establish a network socket connection with either the assigned IP address when run from external to the SecureSync or with the local host address when run from within the time server. This address is set by DNS, unless DNS times-out. This DNS timeout can take longer than the NTPD time-out. So NTPQ can't provide the requested data.
  - Per Oleg: this issue not likely to cause browser/ssh to stop responding.

---

## Time correction associated System logs

time reset +300784145.312704 (note the numeric value of seconds at the end will vary):

From link above: “The time error exceeds the step threshold and has been reset to the correct time.

NTP resets its time by this number of seconds with a “time step”, because the time error was greater than the step threshold of 128 milliseconds. If the time error had been less than 128 milliseconds, the time error would have instead been corrected by slew.

This entry is likely due to the System Time being manually set to an incorrect date/time, so the time was too far off when NTP synced to a valid reference. (Review the Journal log to see if there are any corresponding “**Set Time for User Reference 0 in slot 0**” entries, which indicate a user had manually changed System Time).

**Note:** Refer to “**Time Reset**” when NTP starts up ([..\CustomerServiceAssistance.pdf](#)) for more details on how NTP initially corrects the time.

---

## time slew ? s

The time error exceeds the step threshold and is being slewed to the correct time. You may have to wait a very long time.

**Note:** Refer to “[Time Reset](#)” when NTP starts up (in NTP for all products) for more details on how NTP initially corrects the time and info how to change it via NTP Expert mode.

---

---

## MYSqL/SQLite (“database”) associated entries

### [system] Failed to write event to the database (NOTD)

- Refer to JIRA SSS-1264 (May 2022)
- Refer to Salesforce cases such as 21129
  - Note from this customer: “This error occurred after a power-cycle reboot that I had to do, due to the unit not responding to SSH or HTTP (but it was still responding to PING)”
- Asserted in System log in at least versions 5.9.5 and below
- No benefit to it being asserted. Its strictly a “nuisance entry’ often misconstrued as an indication of a bigger issue occurring.
- I believe it was Ron Dries who said this entry is the direct result of the full SQL database, at one time long ago, being replaced by the sqlite database. Whereas the mysql database could write more than one piece of data at the same time, sqlite can only write one thing at a time. whenever it’s sent more than one thing at a time to be written, this “nuisance” entry is asserted.

---

---

## Apache Web browser associated entries

### [webui] ERROR (4) - ERROR in KTSAL\_Get: SPEC\_KTSAL... entrtird

Examples

[webui] ERROR (4) - ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true XO\_GetMfrMdl 0 (KTSAL)

[webui] ERROR (4)-ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN = true SS\_GetSync 0 (KTSAL)

- Refer to Salesfore case 232901

**Email from Ron Dries (18 May 2020)** The Error(4) message in the system log is harmless.

Periodically we gracefully restart apache, if this occurs while the UI is open and polling the system for status the call will timeout because apache is being restarted and this log message will occur.

- Refer to Salesforce case 23448.

**Email from Paul Myers:** The (4) indicates a process was killed because it received a signal. This can happen if the Web server kills process you are shutting down or rebooting. It could happen in theory because a command took longer than 30 sec and was killed by a timeout in the parent.

(internal use, 31 oct 16) Paul indicated the error (4) entries used to be masked in earlier versions. He unmasked them to see how often they are really asserted and they are not sure exactly why these infrequent alarms occur “out of the blue” He and Ron indicated this entry may be related to a call being placed when the web browser is being closed/timing-out,preventing it from being able to complete,

**Note: graceful restarts of Apache are logged in the error.log file (example below)**

[Tue Jun 01 01:57:26 2021] [notice] Graceful restart requested, doing restart

---

---

## Other System log entries

## “System Time Message” function (STMD)

### “[system] Error: sendto call failed (STMD)”

- Refer to Salesforce cases such as 20728
- Refer also to “System Time Message function” in this same document

[system] Error: sendto call failed (STMD)  
Spectracom last message repeated 31 times  
Spectracom last message repeated 61 times  
Spectracom last message repeated 61 times  
Spectracom last message repeated 11 times

**Q email from Dave L (26 Sept 2019)** I have a PSP GOLD replacement unit we are setting up to go to NYC PD. They have given us a configuration file to pre-load in the unit and after I load the conf file the system log starts producing many of these sendto call failed (STMD) messages:

|    |                 |          |                                  |
|----|-----------------|----------|----------------------------------|
| 96 | Sep 26 16:58:10 | message  | repeated 34 times                |
| 95 | Sep 26 16:57:36 | message  | repeated 31 times                |
| 94 | Sep 26 16:57:05 | [system] | Error: sendto call failed (STMD) |

When I set the configs back to defaults these messages stop.  
What do these sendto call failed (STMD) mean?

**A Reply from Stuart (26 Sept 2019):** They may have saved the config file from a v5.7.1 unit. I turned off System Time Message and the errors stopped logging.

---

## [WEB] Log Feature Failed to read OFDF or RMNF (WEB)

- Refer to Salesforce case 20365 (Kaiser)
- Observed with SecureSync that was running version 5.2.0 software
- Kern log also contained “hda” error messages such as :

```
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=87817,
sector=87817
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8
Jan 12 18:23:10 cdcntp202 kernel: end_request: I/O error, dev hda, sector 87817
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049,
sector=88049
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8
Jan 12 18:23:10 cdcntp202 kernel: end_request: I/O error, dev hda, sector 88049
Jan 12 18:24:37 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:24:37 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049,
sector=88049
```

**Email from Paul Myers (13 Jan 2016)** I may have commented on this before keith, but this unit looks like 2 issues.

Possibly the mysql database is not working write for some errors, but the 2<sup>nd</sup> errors you point out give me concern the CompactFlash is corrupted or worst case the interface to the CF in hardware is causing errors.

You could reboot and clean and see what happens.

OR you could do a clean update.

If the errors exist below then you might have a bad CF or ATA CF interface in hardware is bad. Most likely CF though.

```
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
```



---

## Osc.log (Oscillator log/oscillator.log)

“XO1” versus “XOS” in osc log entries

Differentiating between “KTS disciplining” (used with all TCXO/OCXOs, and with Rb oscillators in v5.8.0 and above) versus Rb oscillator internally disciplining itself (in versions 5.7.x and below)

### E) TCXO/OCXO disciplining (all versions)

F) “xo1” is annotated in all TCXO/OCXO Osc log entries: (indicates TCXO/OCXO is being disciplined using KTS software)

- Example entry with KTS disciplining (5.8.0 and above)

➤ Jun 19 07:11:04: [system] 2015 170 07:11:04 000 **XO1**: Frequency error recalculated: -00.000332 (-3.328x10<sup>-12</sup>)

---

### G) Standard Rubidium oscillator disciplining and LPN Rb (Rb and OCXO) oscillator disciplining

#### 1. Software version 5.8.0 (and above)

➤ changed from Rb disciplining itself, to using the same disciplining as OCXO/TCO (KTS disciplining)

- **(5.8.0 and above) “xos” now annotated in Rb osc log entries:** indicates original disciplining (Rb disciplines itself) in 5.7.x and below

- Example entry with Rb disciplining itself from v (5.7.x and below)

**Apr 29 15:56:14 [system] 2018 119 15:56:13 000 XOS:** Frequency error recalculated: -00.000005 (-5.194x10<sup>-13</sup>)

2. **(5.7.x and below) “xo1” was being annotated in Rb osc log entries:** indicates Rb is disciplined using KTS (like OCXOs and TCXOs)

- Example entry with KTS disciplining (5.8.0 and above)

**Jun 19 07:11:04: [system] 2015 170 07:11:04 000 XO1:**

---

#### 3. LPN Rb (Rb oscillator provides its 10 MHz to OCXO):

➤ Per Dave Sohn, the osc.log reports DAC/1PPS Phase Errors and other calculations for both the Rb and OCXO oscillators installed.

#### a) Example entries from 5.8.9 (reports of high phase errors on case 237264)

**While still at 5.8.4**

Jun 23 09:51:14 2020 175 09:51:14 000 XO1: Freq error: phase start: -105965.3 ns, phase end: -37743.2 ns  
Jun 23 09:51:14 2020 175 09:51:14 000 XO1: Frequency error recalculated: 00.208212 (2.082x10<sup>-08</sup>)  
Jun 23 09:53:29 2020 175 09:53:29 000 XO1: Freq error: phase start: -37743.2 ns, phase end: +23347.3 ns  
Jun 23 09:53:29 2020 175 09:53:29 000 XO1: Frequency error recalculated: 00.000370 (3.703x10<sup>-11</sup>)  
Jun 23 09:53:43 2020 175 09:53:42 000 XOS: Frequency error recalculated: -00.006200 (-6.200x10<sup>-10</sup>)  
Jun 23 10:17:21 2020 175 10:17:21 000 XO1: Freq error: phase start: -37743.2 ns, phase end: -105611.9 ns  
Jun 23 10:17:21 2020 175 10:17:21 000 XO1: Frequency error recalculated: 01.231074 (1.231x10<sup>-07</sup>)  
Jun 23 10:21:15 2020 175 10:21:15 000 XO1: Freq error: phase start: -105611.9 ns, phase end: +269.9 ns  
Jun 23 10:21:15 2020 175 10:21:15 000 XO1: Frequency error recalculated: 00.000213 (2.136x10<sup>-11</sup>)  
**Jun 23 10:21:59 2020 175 10:21:58 000 XOS:** Frequency error recalculated: 00.005324 (5.324x10<sup>-10</sup>)  
Jun 23 10:42:52 2020 175 10:42:52 000 XO1: Freq error: phase start: -105611.9 ns, phase end: -37929.3 ns

Jun 23 10:42:52 175 10:42:52 000 XO1: Frequency error recalculated: 00.208814 (2.088x10^-08)  
Jun 23 10:45:07 2020 175 10:45:07 000 XO1: Freq error: phase start: -37929.3 ns, phase end: +23157.0 ns  
Jun 23 10:45:07 2020 175 10:45:07 000 XO1: Frequency error recalculated: 00.000370 (3.703x10^-11)  
Jun 23 10:45:27 2020 175 10:45:26 000 XOS: Frequency error recalculated: -00.005014 (-5.014x10^-10)  
Jun 23 11:08:59 2020 175 11:08:59 000 XO1: Freq error: phase start: -37929.3 ns, phase end: -105867.5 ns  
Jun 23 11:08:59 2020 175 11:08:59 000 XO1: Frequency error recalculated: 01.231903 (1.231x10^-07)  
Jun 23 11:12:53 2020 175 11:12:53 000 XO1: Freq error: phase start: -105867.5 ns, phase end: +9.6 ns  
Jun 23 11:12:53 2020 175 11:12:53 000 XO1: Frequency error recalculated: 00.000213 (2.136x10^-11)  
Jun 23 11:13:11 2020 175 11:13:10 000 XOS: Frequency error recalculated: -00.000769 (-7.692x10^-11)

Jun 23 13:45:59 Spectracom Spectracom: [spupdate] Application 5.8.4 5.8.9 Upgrade Needed (SWUE)

**After updating 5.8.4 to 5.8.9**

Jun 23 14:41:48 2020 175 14:41:48 000 XO1: Freq error: phase start: +139800.1 ns, phase end: -341.5 ns  
Jun 23 14:41:48 2020 175 14:41:48 000 XO1: Frequency error recalculated: 00.000171 (1.712x10^-11)  
Jun 23 14:50:47 2020 175 14:50:46 000 XOS: Frequency error recalculated: -00.001572 (-1.572x10^-10)  
Jun 23 15:02:55 2020 175 15:02:55 000 XO1: Freq error: phase start: +139800.1 ns, phase end: -72141.7 ns  
Jun 23 15:02:55 2020 175 15:02:55 000 XO1: Frequency error recalculated: 00.281040 (2.810x10^-08)  
Jun 23 15:05:34 2020 175 15:05:34 000 XO1: Freq error: phase start: -72141.7 ns, phase end: +400.5 ns  
Jun 23 15:05:34 2020 175 15:05:34 000 XO1: Frequency error recalculated: 00.000314 (3.144x10^-11)  
Jun 23 15:07:27 2020 175 15:07:26 000 XOS: Frequency error recalculated: 00.014160 (1.415x10^-09)  
Jun 23 15:27:11 2020 175 15:27:11 000 XO1: Freq error: phase start: -72141.7 ns, phase end: -32373.9 ns  
Jun 23 15:27:11 2020 175 15:27:11 000 XO1: Frequency error recalculated: 00.402711 (4.027x10^-08)  
Jun 23 15:29:26 2020 175 15:29:26 000 XO1: Freq error: phase start: -32373.9 ns, phase end: +29223.8 ns  
Jun 23 15:29:26 2020 175 15:29:26 000 XO1: Frequency error recalculated: 00.000370 (3.703x10^-11)  
Jun 23 15:29:43 2020 175 15:29:42 000 XOS: Frequency error recalculated: -00.008330 (-8.330x10^-10)  
Jun 23 15:53:18 2020 175 15:53:18 000 XO1: Freq error: phase start: -32373.9 ns, phase end: -93781.8 ns  
Jun 23 15:53:18 2020 175 15:53:18 000 XO1: Frequency error recalculated: 01.173534 (1.173x10^-07)  
Jun 23 15:56:44 2020 175 15:56:44 000 XO1: Freq error: phase start: -93781.8 ns, phase end: +217.0 ns  
Jun 23 15:56:44 2020 175 15:56:44 000 XO1: Frequency error recalculated: 00.000242 (2.427x10^-11)  
Jun 23 15:57:27 2020 175 15:57:26 000 XOS: Frequency error recalculated: 00.004116 (4.116x10^-10)  
Jun 23 16:18:21 2020 175 16:18:21 000 XO1: Freq error: phase start: -93781.8 ns, phase end: -32591.7 ns  
Jun 23 16:18:21 2020 175 16:18:21 000 XO1: Frequency error recalculated: 00.167277 (1.672x10^-08)  
Jun 23 16:20:36 2020 175 16:20:36 000 XO1: Freq error: phase start: -32591.7 ns, phase end: +29018.2 ns  
Jun 23 16:20:36 2020 175 16:20:36 000 XO1: Frequency error recalculated: 00.000370 (3.703x10^-11)  
Jun 23 16:20:54 2020 175 16:20:54 000 XOS: Frequency error recalculated: -00.005468 (-5.468x10^-10)  
Jun 23 16:44:28 2020 175 16:44:28 000 XO1: Freq error: phase start: -32591.7 ns, phase end: -94040.9 ns  
Jun 23 16:44:28 2020 175 16:44:28 000 XO1: Frequency error recalculated: 01.174426 (1.174x10^-07)  
Jun 23 16:47:55 2020 175 16:47:55 000 XO1: Freq error: phase start: -94040.9 ns, phase end: +428.0 ns  
Jun 23 16:47:55 2020 175 16:47:55 000 XO1: Frequency error recalculated: 00.000241 (2.415x10^-11)  
Jun 23 16:48:39 2020 175 16:48:38 000 XOS: Frequency error recalculated: 00.004230 (4.230x10^-10)

~~~~~

b) Example entries from a different 5.8.8 SecureSync for comparison

Apr 5 17:31:20 2018 095 17:31:19 000 XO1: Initial DAC Setting: 0x6E71
Apr 5 17:31:20 2018 095 17:31:19 000 XO1: Saved Cal Value: H/S:+0.0002946644
Apr 5 18:10:16 2018 095 18:10:15 000 XO1: Initial DAC Setting: 0x6E71
Apr 5 18:10:16 2018 095 18:10:15 000 XO1: Saved Cal Value: H/S:+0.0002946644
Apr 9 14:29:17 2018 099 14:29:17 000 XO1: Initial DAC Setting: 0x6E71
Apr 9 14:29:17 2018 099 14:29:17 000 XO1: Saved Cal Value: H/S:+0.0002946644
Apr 9 18:52:02 000 XO1: Initial DAC Setting: 0x6E71
Apr 9 18:52:02 XO1: Saved Cal Value: H/S:+0.0002946644
Apr 9 20:22:51 XO: Ref Changed: old=none new=hst0
Apr 9 20:22:52 XO: Phase Reference Valid.
Apr 9 20:24:53 XO1: Initial DAC Setting: 0x6E71
Apr 9 20:24:53 2018 099 20:24:53 000 XO1: Saved Cal Value: H/S:+0.0002946644
Apr 9 20:46:27 2018 099 20:46:22 000 XO: Ref Changed: old=none new=hst0
Apr 9 20:46:27 2018 099 20:46:22 000 XO: Phase Reference Valid.

Apr 9 20:48:28 2018 099 20:48:29 000 XO1: Initial DAC Setting: 0x6E71
Apr 9 20:48:28 2018 099 20:48:29 000 XO1: Saved Cal Value: H/S:+0.0002946644
Jun 21 15:36:19 2018 172 15:36:14 000 XO: Ref Changed: old=none new=hst0
Jun 21 15:36:19 2018 172 15:36:14 000 XO: Phase Reference Valid.
Jun 21 15:38:13 2018 172 15:38:13 000 XO1: Initial DAC Setting: 0x6E71
Jun 21 15:38:13 2018 172 15:38:13 000 XO1: Saved Cal Value: H/S:+0.0002946644

Minor Issue with oscillator log (decimal point one place off)

- Refer to Salesforce case 19963 / Mantis case 3177
- At least 5.3.0 and 5.3.1 have the decimal place in the numeric frequency error one place too far to the right
 - Instead of “0.0”, it’s being displayed in the log entry as “00.0” (need to move it one place to the left to be correct).
 - Scientific notation value is correct. Just displaying decimal point in the wrong location.

Harris software only (such as version 5.4A)

- Refer to salesforce case 25697
 - Jun 18 01:52:58 S12u2clk S12u2clk: [system] 2017 169 01:52:58 000 XO: Ref Changed: old=gps0 new=gps0
 - Jun 18 01:52:59 S12u2clk S12u2clk: [system] 2017 169 01:52:58 000 XO: Phase Reference Invalid.
 - Jun 18 01:53:00 S12u2clk S12u2clk: [system] 2017 169 01:52:59 000 XOS: Rb track off -- free run
 - Jun 18 01:53:16 S12u2clk S12u2clk: [system] 2017 169 01:53:16 000 XO: Ref Changed: old=gps0 new=gps0
 - Jun 18 01:53:16 S12u2clk S12u2clk: [system] 2017 169 01:53:16 000 XO: Phase Reference Valid.
 - Jun 18 01:54:51 S12u2clk S12u2clk: [system] 2017 169 01:54:50 000 XOS: Rb synchronized

Oscillator Calibration log entries- Refer to: [Oscillator Calibration log entries](#)

Note: Software version 5.1.7 added **several** improvements to TCXO/OCXO disciplining.

“New Cal Value”: Only happens at factory or if a patch is applied to reset it. This entry can be eventually overwritten.

“Saved Cal Value”: The previously calculated value stored in the EEPROM.

“phase start” and “phase end” entries in the Oscillator log

Sep 17 00:02:15 clock.l4.eexchange.com clock.l4: [system] 2015 260 00:02:15 000 XO1: Freq error: phase start: +20.4 ns, phase end: +45.0 ns

- I believe these entries started being added to Oscillator log in upgrade version 5.2.1 (they are in v5.2.1, but may have been added earlier).
- Periodically logs the 1PPS phase error measurement.

Email Keith sent (17 Sept 15) Instead of SecureSync just reporting in the web browser the 1PPS phase error (which is the measured offset between the 1PPS input reference and the unit’s internal System 1PPS) newer software versions now also periodically log this value in the Oscillator log. These are reported as “phase start” and “phase end”. The lower the 1PPS phase error, the more accurate the SecureSync is to its external reference (with a Rubidium oscillator installed, these values will typically be less than around 100ns).

Err Mean / Standard deviation

- Group of entries for TXCO/OCXO oscillators asserted after every time Disciplining qualifies/locks the oscillator

Examples from our Customer Service.176 at version 5.1.7. OCXO (5ppb) oscillator

13:44:28 Custservice Custservice.176: [system] 2014 308 13:44:28 000 XO1: Initial DAC Setting: 0x8C54
Nov 4 13:44:28 Custservice Custservice.176: [system] 2014 308 13:44:28 000 XO1: Saved Cal Value: H/S:+0.0001377126
Nov 4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: DAC Setting: 0x8C42
Nov 4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Phase Err: +25.0
Nov 4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Freq Err: +0.004166
Nov 4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Err Chg Mean: +0.3
Nov 4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Err Chg Std Dev: +5.6

Several examples from our Customer Service.176 at version 5.1.6 or lower. OCXO (5ppb) oscillator

Oct 13 11:15:35 Custservice Custservice.176: [system] 2014 286 11:15:35 000 XO1: Initial DAC Setting: 0x8CAD
Oct 13 11:15:35 Custservice Custservice.176: [system] 2014 286 11:15:35 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 17 16:36:32 Custservice Custservice.176: [system] 2014 290 16:36:32 000 XO1: Initial DAC Setting: 0x8BC2
Oct 17 16:36:32 Custservice Custservice.176: [system] 2014 290 16:36:32 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 17 16:45:31 Custservice Custservice.176: [system] 2014 290 16:45:31 000 XO1: Initial DAC Setting: 0x8BC2
Oct 17 16:45:31 Custservice Custservice.176: [system] 2014 290 16:45:31 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 20 12:02:05 Custservice Custservice.176: [system] 2014 293 12:02:05 000 XO1: Initial DAC Setting: 0x8BC2
Oct 20 12:02:05 Custservice Custservice.176: [system] 2014 293 12:02:05 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 24 21:35:24 Custservice Custservice.176: [system] 2014 297 21:35:25 000 XO1: Initial DAC Setting: 0x8BC2
Oct 24 21:35:25 Custservice Custservice.176: [system] 2014 297 21:35:25 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 28 15:56:14 Custservice Custservice.176: [system] 2014 301 15:56:13 000 XO1: Initial DAC Setting: 0x8BC2
Oct 28 15:56:14 Custservice Custservice.176: [system] 2014 301 15:56:13 000 XO1: Saved Cal Value: H/S:+0.0001377126
Oct 28 16:33:44 Custservice Custservice.176: [system] 2014 301 16:33:59 000 XO1: Err Mean: -1.5
Oct 28 16:33:44 Custservice Custservice.176: [system] 2014 301 16:33:59 000 XO1: Err Std Dev: +5.9

Hi / Lo / Referr entries

- This group of entries are asserted each time system switches from Holdover back to a Reference

Per Dave Sohn (30 Jan 2014) : These are logged results from the reference qualification coming back from holdover”.

(Refer to entries below in red)

Dec 28 15:49:49 COLW-SecureSync COLW-SecureSync: [system] 2013 362 15:49:49 000 XO1: Frequency error recalculated:
00.0000030 (3.043x10⁻¹³)
Dec 28 16:06:59 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:06:59 000 XO1: Frequency error recalculated:
00.0001917 (1.917x10⁻¹¹)
Dec 28 16:24:52 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:24:52 000 XO1: hi= +195.0
Dec 28 16:24:52 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:24:52 000 XO1: lo= -135.0
Dec 28 16:24:52 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:24:52 000 XO1: RefErr= +165.0
Dec 28 16:27:04 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:27:04 000 XO1: hi= +40.0
Dec 28 16:27:04 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:27:04 000 XO1: lo= -40.0
Dec 28 16:27:04 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:27:04 000 XO1: RefErr= +40.0
Dec 28 16:31:36 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:31:36 000 XO1: Frequency error recalculated:
00.0004376 (4.376x10⁻¹¹)
Dec 28 16:53:18 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:53:18 000 XO1: Frequency error recalculated:
00.0000071 (7.177x10⁻¹³)

“Frequency Error recalculated” messages

- Entries only asserted if an external reference that can discipline the oscillator is present/valid
- Typical values for good OCXO, when locked to GPS: no worse than around “ 5.994×10^{-11} ”

Spectracom SecureSyncs contain one of five types of internal 10 MHz oscillators. The internal oscillator is used to output 10 MHz and to generate an internal 1PPS signal.

The “Oscillator” log provides an indication of the frequency counts of the oscillator’s 10 MHz output, as measured using the selected 1PPS Input Reference (Such as a GPS receiver’s 1PPS output signal) as a reference.

The “**frequency error recalculated**” messages in this log indicate the accuracy of the oscillator output, in comparison to a perfect 10 MHz signal (known as the “**fractional frequency error**”). The 10 MHz oscillator output is measured against the 1PPS generated by the selected 1PPS input reference.

H) Newer browser

Id	Date	Entity	Message
157	Aug 14 14:35:13	[system]	2015 226 14:35:13 000 XO1: Frequency error recalculated: -00.001021 (-1.021x10^-11)

The phrase “FREQUENCY ERROR RECALCULATED” designates the value to follow is reporting how close the oscillator’s actual 10 MHz output signal is to the desired frequency of 10.0000000 MHz (reported in scientific notation). This phrase is not an indication that there is a problem with the oscillator.

I) Classic interface

LOG FILES			
Timestamps are in system timescale (UTC)			
Event	Alarm	Oscillator	GPS Qualification
Jan 7 15:23:48	Spectracom Spectracom	[system] 2013 007 15:23:47 000 XO1	Frequency error recalculated: 00.0000000 (7.816x10^-11)
Jan 7 15:06:37	Spectracom Spectracom	[system] 2013 007 15:06:37 000 XO1	Frequency error recalculated: 00.0000784 (7.848x10^-12)
Jan 7 14:48:28	Spectracom Spectracom	[system] 2013 007 14:48:27 000 XO1	Frequency error recalculated: 00.0001319 (1.319x10^-11)
Jan 7 14:32:17	Spectracom Spectracom	[system] 2013 007 14:32:17 000 XO1	Frequency error recalculated: 00.0000204 (2.041x10^-12)

The phrase “FREQUENCY ERROR RECALCULATED” designates the value to follow is reporting how close the oscillator’s actual 10 MHz output signal is to the desired frequency of 10.0000000 MHz (reported in scientific notation). This phrase is not an indication that there is a problem with the oscillator.

Important Note- The “FREQUENCY ERROR RECALCULATED” phrases displayed on this web page DO NOT mean a problem exists with either the internal oscillator or with the NTP server. “FREQUENCY ERROR RECALCULATED” refers to the Fractional Frequency Error which is a comparison of the actual output frequency versus the desired frequency (The desired frequency is 10.0000000 MHz), reported in scientific notation. This phrase will ALWAYS be present on this page to show the measured 10 MHz frequency. If a problem DOES happen to exist with the oscillator frequency measurements, a Frequency alarm will be entered in the “Alarms” log.

The lower the “Frequency error recalculated” value is, the closer the oscillator is to outputting an exact 10 MHz signal. Below is a table of the 10MHz specifications. The “Frequency error calculated” values should typically be less than the values in the “Short term Stability” section of this table, for the specific type of oscillator installed, as long as SecureSync is synced to an external reference (other than other NTP servers).

10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy (average over 24 hours when GPS locked)	1x10 ⁻¹¹	2x10 ⁻¹²	1x10 ⁻¹²	1x10 ⁻¹²	1x10 ⁻¹²
Medium Term Stability (without GPS after 2 weeks of GPS lock)	1x10 ⁻⁸ /day	5x10 ⁻¹⁰ /day	2x10 ⁻¹⁰ /day	5x10 ⁻¹¹ /month (3x10 ⁻¹¹ /month typical)	5x10 ⁻¹¹ /month (3x10 ⁻¹¹ /month typical)
Short Term Stability (Allan variance)					
1 SEC	2x10 ⁻⁹	5x10 ⁻¹⁰	5x10 ⁻¹¹	2x10 ⁻¹¹	5x10 ⁻¹⁰
10 SEC	1x10 ⁻⁹	5x10 ⁻¹¹	2x10 ⁻¹¹	2x10 ⁻¹²	2x10 ⁻¹¹
100 SEC	3x10 ⁻¹⁰	1x10 ⁻¹¹	1x10 ⁻¹¹	2x10 ⁻¹²	5x10 ⁻¹²

“Frequency error recalculated: 00.0000000 (0.000x10⁻¹⁶)” (0.000e-16 or 0.000x10-16)

Note: This oscillator.log entry can be asserted for one of two reasons:

A) The actual frequency error is less than we can measure

Email from Dave Sohn (27 Jan 15) after I alluded to the software issue below It is still possible to receive a frequency error of 0 if it is below our measurement capability. We fixed where negative frequency errors were reported as 0.

Edited Email Keith sent to Masataka (27 Jan 15)

Thanks for forwarding along your customer’s inquiry about the oscillator log entries.

The oscillator log entry of “**Frequency error recalculated: 00.000000 (0.000x10⁻¹⁶)**” is not a symptom of any problems occurring with the SecureSync. These log entries just mean that the magnitude of the frequency error at that time was less than the threshold that the system can even measure. In this case, the Frequency Error is reported as “0.000x10⁻¹⁶” (the lowest value possible for the system to report). So instead of these log entries being a symptom of a problem, they instead indicate the oscillator is as close to being at the desired frequency as the system is capable of measuring.

B) A minor software issue in software versions 5.10 through 5.1.4 (fixed in 5.1.5)

- Software issue with reporting the frequency error in the Oscillator log
- Negative values were being incorrectly being reported as “0” (“So any negative frequency error measurements will show as 0.000x10-16.”)
- Refer to Mantis case 2862 <http://cvsmantis.int.rolia.com/mantis/view.php?id=2862>
- This issue first started in version 5.1.0.
- Fixed in version 5.1.5 software update

Software version 5.1.4 improvements to oscillator disciplining

Email from Dave Lorah to Masataka (24 June 2014) As far as changes between 5.0.2 and 5.1.4, we improved our measurement window adjustments, improved our initial sync time performance, and added adjustable filtering based on input reference error. There would be a difference in the oscillator log measurements due to these changes. The oscillator measurement range should be in the x10-11 to x10-13 range. The oscillator log you sent us shows typical performance.

Rb Reference unstable

Per Dave Sohn, this entry indicates the Rb oscillator was forced into free-run due to issues with the selected 1PPS reference (system itself doesn't go into Holdover mode. But the oscillator is in free-run. Another entry is asserted "Rb synchronized" once the oscillator is relocked with the 1PPS reference.

- This entry could potentially indicate a bad Rb oscillator, but is more likely caused by issues with the selected 1PPS reference (such as issues with a Res-SMT-GG receiver, including earlier firmware versions, such as 1.6 and 1.7)

Diagnosing this entry

1. Also review the **discstats** entries (in addition to the other system logs) for additional info on operation of the oscillator when this entry is asserted. In **discstats**, look for likely large increases in the frequency error measurements (such as normally around 1×10^{-13} , but then they change to a larger value such as 1×10^{-10} (which was observed in Salesforce case 20249 also mentioned below).
2. The "Rb Reference unstable" alarm has been seen in one case where no other log entries were asserted in other logs- Alarms, Timing, Events, etc. and reception was fine. Refer to Salesforce case 20249.
3. The "Rb Reference unstable" alarm has been seen correlated with the following entry in the Timing log (Res-SMT-GG firmware issue)

"[system] 2014 291 13:01:08 002 Error: CS_Set(CS_SA_LEAP_SEC) call from GR."

Rb peak voltage error alarms

- Also refer to: "SRO-100 Rubidium oscillators" in the Customerserviceassistance document

Note: Archive software versions 5.0.0 and below reported all alarms associated with the Rubidium oscillator as "Rb peak voltage error" alarms. This was noticed just prior to the version 5.0.1 release, so version 5.0.1 now differentiates each Rb oscillator alarm to indicate what the real issue with the Rb oscillator.

Q. (log entry from Morgan Stanley Rb-based SecureSync) **Rb peak voltage error** (val=6, min=51, max=255)

A (1/25/12) Mark Goodlein emailed SpectraTime with: We have a customer with one of our SecureSync products, in which we use an SRO-100 Rubidium oscillator module. Recently, this customer saw some behavior that was questionable and would like to know if they should be concerned about it.

Our software that communicates with the SRO requests the internal parameters using the 'M' command once a second. It then compares the values returned with boundary values to detect if something is out of the ordinary, in which case we log the condition. This customer's unit had been running for over 150 days then the following log messages were recorded for 5 seconds then went away and no more have been logged since then.

```
2011 357 21:26:54 000 Rb peak voltage error (val=6, min=51, max=255)
2011 357 21:26:55 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:56 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:57 000 Rb peak voltage error (val=9, min=51, max=255)
2011 357 21:26:58 000 Rb peak voltage error (val=35, min=51, max=255)
```

The manual for the SRO indicates that this signal stabilizes to between 1 and 5 volts after warm-up, so these are the boundary conditions that our software checks for. In this case, the voltage dipped below 1V (almost reaching 0V) for 5 seconds. This is the first case of an event like this that has ever been reported to us from a customer.

Is this event something to be concerned about? Does it indicate a condition that may result in failure?

Oscillator Log entries associated with Wenzel oscillator's PLL lock status

- Refer to the CGU manual addendum for Hughes (1200-5000-C050) in Arena at: https://app.bom.com/items/detail-spec?item_id=1217182411&version_id=10446313248&orb_msg_single_search_p=1

- Also refer to [Options/Specials](#) in this doc (scroll down to the Hughes CGU)

Example entries in the osc.log

```
[system] PLL_0 Lock Error (KAD)
[system] PLL_0 Lock Good (KAD)
[system] PLL_1 Lock Error (KAD)
[system] PLL_1 Lock Good (KAD)
```

Example entries in osc.log

91	Nov 03 00:31:48	[system]	PLL_1 Lock Error (KAD)
90	Nov 03 00:31:48	[system]	PLL_0 Lock Error (KAD)
89	Nov 03 00:31:30	[system]	PLL_0 Lock Good (KAD)
88	Nov 03 00:30:47	[system]	PLL_1 Lock Good (KAD)
85	Nov 03 00:13:39	[system]	PLL_1 Lock Error (KAD)
84	Nov 03 00:09:10	[system]	PLL_0 Lock Error (KAD)

(Non-Wentzel oscillator SecureSyncs) Note PLL_0 Lock Error (KAD) / PLL_1 Lock Error (KAD) entries have also been observed on non-wentzel oscillator configuration.

- In at least case (case 262649) it appears it can happen if the KTS version isn't the correct version for the CFcard version installed (such as replacing the CF Card without then applying a software update)
- Based on a few other cases (such as 203789 and 284051) appears these entries can simply be another indication the Rb oscillator is failing/has failed (not meaning anything different).

Raccon.log (rc log)

- I believe this may be a Radius log, but not positive

Qual.log entries (Qual log)

- GPS reception - Refer to: I:\Customer Service\GPS\GPS reception Ap Notes\SecureSync for a description of this log.

Reboot/power cycle of the unit erases the Qual log data before the reboot occurred (since the top of the current hour)

- Qual log data is only written to the log 2 seconds after the end of each hour
- If a reboot/power cycle occurs after the beginning of the hour, the data between the beginnings of the hour until the reboot occurred is lost. So the Qual log will only report the data from the power-up until the end of that hour (Q will not include any data in the current hour before the power cycle occurred).

Issue with GNSS receiver dropping to 0 sats

- Applicable in at least version 5.1.4 software.
- Refer to Deviation (ECN) 3481

Email from Dave West (20 May 2014) The GNSS Receiver has an error with the following:

If GPS tracks randomly 0 Satellites for 1 to 5 seconds, this is a known bug.

It is acceptable for the units that display this to ship.

This Deviation is in place until the next release later than 5.1.4

Test Procedure 1200-XXXX-0600-TP was updated to include this deviation and is now at revision 19

Havequick input (no GPS input)

- Loss/regain of GPS reception causes “QR hvq0” log entries to be asserted.

Sep 20 15:10:14 Timeserver2 Timeserver2: [system] 2013 263 15:10:14 000 QR hvq0 has lost communication.

Sep 20 15:10:15 Timeserver2 Timeserver2: [system] 2013 263 15:10:15 000 QR hvq0 has established communication.

Email from Dave Sohn (21 Jan 2014) If the signal is disconnected or lost, these messages will appear and return. This is not a system alarm.

- Used in conjunction with the rexd.log
- This system log is not accessible from the browser. But it's in the Save Logs bundle.
- This log is not wiped when performing a “clear all logs” in the browser
- Rxd.log was added in software version 5.0.2
- This log is not viewable from the web browser (can FTP it out as a single log, bundle it with all of the logs or view it with telnet/ssh)

Jun 12 14:39:07 [NOTE] Found gps receiver
Jun 12 14:39:07 [NOTE] rexd.sh has started
Jun 13 02:55:01 [HANDLER] nullmailer clean up successful

- These entries are normal and expected, starting in v5.1.2 (as a fix to the nullmailer issue filling logs)
- Refer to Mantis case 2390 (~Oct 2013)
- Linux OS messages get queued (in nullmailer package) to be sent out for every log entry. The recipient email address is not filled out and the queue folder is growing since it cannot send messages out.
- Per the Mantis case, there is now a script to empty the folder every 5 hours. These entries indicate it was successfully cleaned up.

“xinetd” log entries in rexd.log

Xinetd: (*extended Internet daemon*) is an open-source super-server daemon which runs on many Unix-like systems and manages Internet-based connectivity.

xinetd listens for incoming requests over a network and launches the appropriate service for that request.^[4] Requests are made using port numbers as identifiers and xinetd usually launches another daemon to handle the request. It can be used to start services with both privileged and non-privileged port numbers.

errno (such as “**errno = 22**” for example)

- Refer to the following website for a list of errno numbers and what they mean: http://www-niumi.fnal.gov/offline_software/srt_public_context/WebDocs/Errors/unix_system_errors.html

For example: “(**errno = 22**)” means “Invalid argument”

xinetd[21807]: socket bind: Invalid argument (errno = 22) : Appears to be a known issue with earlier versions of xinetd. Updating SecureSync to a newer version is likely to prevent these entries.

xinetd[7302]: Failed to contact identity server at ::ffff:10.14.104.11: system error

(Identity Integration server / MIIS) synchronize identity information from many different directories and services into a single, organization-wide solution. This can help protect your network's security and simplify management.

“telnetd” (telnet) log entries in rexd.log

telnetd[24923]: tloop: peer died: EOF

- Due to an abrupt loss of telnet connection
- Can be caused by not exiting the connection before closing out, for example.

Below is from a Google search

But guessing that you see it in a telnetd log it could be something innocent like somebody connected using telnet and instead of logging out they just clicked the x in the top corner of the app to shut it down. Or the telnet app crashed or their computer crashed or lost network connectivity. All the telnetd app knows is that it was talking to someone and then that connection was lost. It could be that someone is scanning your computer to see if you are running telnet on any ports so that they can try to hack you. I am a little surprised that you are running telnet since everyone I know has banned it from their network and uses ssh instead.

GPS monitor logs in rexd.log

Oct 18 14:18:08 [RESTART] Restarting initiated for gpsmond

- GPS monitor likely reset due to a software issue with version 5.0.2, when no GPS receiver is installed. (There will be several of these entries in this log).

SNMP log entries in rexd.log

SNMP automatically restarting (snmpsad)

[RESTART] Restarting initiated for snmpsad
[RESTART] Restarting initiated for snmpsad
[SUCCESS] Successfully restarted snmpsad

- SNMPSAD being restarted automatically if it crashed was added in version 5.1.3.
- SNMP likely restarted by rexd because of walking the MIBs with the timeout value being set too low for the NTP

associated objects. Timeout should be set to a minimum of about 9 to 10 seconds.

Nullmailer log entries in rexd.log

Lots of [HANDLER] nullmailer clean up successful entries asserted

Jun 14 02:47:13 [HANDLER] nullmailer clean up successful

Jun 14 15:06:50 [HANDLER] nullmailer clean up successful

Jun 15 03:27:02 [HANDLER] nullmailer clean up successful

Jun 15 15:46:42 [HANDLER] nullmailer clean up successful

Jun 16 04:06:29 [HANDLER] nullmailer clean up successful

- These entries are normal and expected, starting in 5.1.2 (as a fix to the nullmailer issue in v5.0.2).
- Refer to Mantis case 2390 (~Oct 2013)
- Email messages get queued (in nullmailer package) to be sent out for every log entry. The recipient email address is not filled out and the queue folder is growing since it cannot send messages out.
- Per the Mantis case, there is now a script to empty the folder every 5 hours. These entries indicate it was successfully cleaned up.

qual.log (Qual log entries)

- Refer to the GPS Reception Tech Note: <I:\Customer Service\GPS\GPS reception Ap Notes\SecureSync>

rc.log (raccoon log)

- Linux start-up and shut-down log????

snmpd.log

- Software update version 5.2.0 updated Net-SNMP from version 5.6.1 to version 5.6.2.1
- This SNMP log is being deprecated (it's being removed from update versions 5.2.1 and above). Refer to Mantis case 3007.

SNMP starting up:

C) SNMP version 5.6.2.1 (software version 5.2.0)

Note: As mentioned above, this log is being removed starting in update v5.2.1 (April 2015)

Turning on AgentX master support.
NET-SNMP version 5.6.1
Reconfiguring daemon

D) SNMP version 5.6.1 (software versions 5.1.7 and below installed)

Turning on AgentX master support.
SNMP version NET-SNMP version 5.6.1

SNMPD log entries either during a software update or with a halt being performed.

Received TERM or STOP signal... shutting down...

Known issues with SNMP (seen in software versions 5.1.7 and below. Should be fixed in 5.2.0 and above)

- "Error expanding HCOOutOctets to 64bits in ipSystemStatsTable.ipv6" and "looks like a 64bit wrap, but prev!=new"
- Observed with version 5.1.5 software installed. Recommend update to v5.2.0 (Jan 2015) or above which includes

SNMP update to newer version (v5.6.2.1)

Info below is from: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/6.1_Technical_Notes/net-snmp.html

BZ#[674757](#)

The snmpd daemon did not properly initialize it's structures for IP-MIB::ipSystemStatsTable and IP-MIB::ipIfStatsTable properly. It returned this error message "looks like a 64bit wrap, but prev!=new" to log if a counter in these tables got larger than 32bits. The updated package fixes initialization of the tables and ensures that the aforementioned message should not appear in snmpd log.

All users of net-snmp are advised to upgrade to these updated packages, which resolve these issues.

Error log (ssl_request_log: Apache web browser's Access log)

- These log entries are from /var/log/apache2/error.log
- Refer to <http://httpd.apache.org/docs/2.2/logs.html> for more info
- Added in software versions 5.2.1 (I believe)
- Logs from Apache's Access log (reported pages that were accessed)
- Starts with ".log.1" as the file extension instead of just ".log" like the other log files
- View this log via CLI or from a log capture file

Format of Access log entries

The format of the access log is highly configurable. The format is specified using a format string that looks much like a C-style printf(1) format string. Some examples are presented in the next sections. For a complete list of the possible contents of the format string, see the [mod_log_config format strings](#).

Common Log Format

A typical configuration for the access log might look as follows.

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

```
CustomLog logs/access_log common
```

This defines the *nickname* common and associates it with a particular log format string. The format string consists of percent directives, each of which tell the server to log a particular piece of information. Literal characters may also be placed in the format string and will be copied directly into the log output. The quote character (") must be escaped by placing a backslash before it to prevent it from being interpreted as the end of the format string. The format string may also contain the special control characters "\n" for new-line and "\t" for tab.

The above configuration will write log entries in a format known as the Common Log Format (CLF). This standard format can be produced by many different web servers and read by many log analysis programs. The log file entries produced in CLF will look something like this:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

Each part of this log entry is described below.

1. 127.0.0.1 (%h)

This is the IP address of the client (remote host) which made the request to the server. If [HostnameLookups](#) is set to On, then the server will try to determine the hostname and log it in place of the IP address. However, this configuration is not recommended since it can significantly slow the server. Instead, it is best to use a log post-processor such as [logresolve](#) to determine the hostnames. The IP address reported here is not necessarily the address of the machine at which the user is sitting. If a proxy server exists between the user and the server, this address will be the address of the proxy, rather than the originating machine.

2. (%l)

The "hyphen" in the output indicates that the requested piece of information is not available. In this case, the information that is not available is the RFC 1413 identity of the client determined by `identd` on the clients machine. This information is highly unreliable and should almost never be used except on tightly controlled internal networks. Apache `httpd` will not even attempt to determine this information unless [IdentityCheck](#) is set to `On`.

3. frank (%u)

This is the userid of the person requesting the document as determined by HTTP authentication. The same value is typically provided to CGI scripts in the `REMOTE_USER` environment variable. If the status code for the request (see below) is 401, then this value should not be trusted because the user is not yet authenticated. If the document is not password protected, this part will be "-" just like the previous one.

4. [10/Oct/2000:13:55:36 -0700] (%t)

The time that the request was received. The format is:

[day/month/year:hour:minute:second zone]

day = 2*digit

month = 3*letter

year = 4*digit

hour = 2*digit

minute = 2*digit

second = 2*digit

zone = (^+|`-') 4*digit

It is possible to have the time displayed in another format by specifying `%{format}t` in the log format string, where `format` is as in `strftime(3)` from the C standard library.

5. "GET /apache_pb.gif HTTP/1.0" (%r)

The request line from the client is given in double quotes. The request line contains a great deal of useful information. First, the method used by the client is `GET`. Second, the client requested the resource `/apache_pb.gif`, and third, the client used the protocol `HTTP/1.0`. It is also possible to log one or more parts of the request line independently. For example, the format string "`%m %U%q %H`" will log the method, path, query-string, and protocol, resulting in exactly the same output as "`%r`".

4. 200 (%>s)

This is the status code that the server sends back to the client. This information is very valuable, because it reveals whether the request resulted in a successful response (codes beginning in 2), a redirection (codes beginning in 3), an error caused by the client (codes beginning in 4), or an error in the server (codes beginning in 5). The full list of possible status codes can be found in the [HTTP specification](#) (RFC2616 section 10).

6. 2326 (%b)

The last part indicates the size of the object returned to the client, not including the response headers. If no content was returned to the client, this value will be "-". To log "0" for no content, use `%B` instead.

Example "normal" entries (from one of our NetClocks)

```
[23/Jul/2015:11:48:58 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Features/getTime HTTP/1.1" 288
[23/Jul/2015:11:49:05 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2053
[23/Jul/2015:11:49:09 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1365
[23/Jul/2015:11:49:15 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/status HTTP/1.1" 105885
[23/Jul/2015:11:49:25 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2053
[23/Jul/2015:11:49:28 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1365
[23/Jul/2015:11:49:42 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2053
```

```
[23/Jul/2015:11:49:46 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1370
[23/Jul/2015:11:49:54 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/status HTTP/1.1" 105961
[23/Jul/2015:11:49:58 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Features/getTime HTTP/1.1" 288
[23/Jul/2015:11:49:59 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2055
[23/Jul/2015:11:50:04 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1365
```

****sys.log entries (Syslog log)**

- This log is not wiped when performing a “clear all logs” in the browser.
- No syslog log available for view in the browser.
 - sys.log can only be viewed via the CLI interface (It’s in the **home/spectracom/logs** directory)
- Contains entries for syslog stopping and starting

Example “normal” entries

“Spectracom syslogd 1.5.0: restart.”: Indicates unit was rebooted.

```
Jan 21 20:06:02 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:06:03 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:06:20 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:06:20 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:11:21 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:11:22 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:16:22 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:16:23 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:21:24 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
```

****system.log entries (and MySQL database)**

A) Version info reported in System log for log reviewing

- Version 5.2.1 update (Apr 2015) added Model and Serial Number to the System Log at each start-up.
- Update Version 5.2.0 added the System /Timing System version info to the system.log after each power-up (for knowing the version when reviewing logs).

B) Fan control/temperature monitoring associated log entries (starting in version 5.3.1)

1. (Starting in v5.3.1 and if the EEPROM has been reprogrammed): On boot, the Fan Control feature detection is logged in the system log.
2. Log entry asserted after each boot-up (starting in v5.3.1) *Temperature Monitor daemon has started (TEMPD)*

C) log entries associated with glitch in or loss of 10MHz into the FPGA (Version 5.2.0 and above)

Event log (just some possible examples)

```
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GR_GetMfrMdl 0 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetState 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetOscType 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetSerialNo 0 (KTSAL)
```

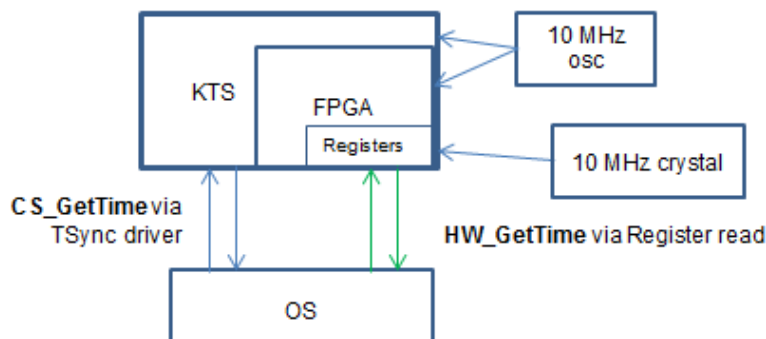
System log

- Timing System Hardware error
- Failed CS_GetTime (KAD)

Then either:

- Passed HW_GetTime (possible oscillator error) (KAD) Or
- Failed HW_GetTime (probably FPGA failure) (KAD)

Details



1. If there are at least five (5) “Failed to read alarm info from KTS (KAD)...” entries in the **System** log, first a “CS_GetTime” call is sent to KTS to see if KTS is still communicating via the TSync driver.
 - If there are less than 5 entries, nothing happens and the counter is reset
 - If there are at least 5 entries, the Tsync driver **will** be unloaded (reboot will be necessary to restore operation)
2. Then a “HW_GetTime” call is sent to the FPGA registers to see if the FPGA is communicating.
 - If this call passes, the registers are still able to respond (if KTS isn’t running, the same data may remain in

the registers). This confirms the TSync driver is still running normally.

- If this call fails, the registers are not able to provide any data whatsoever. This means either bad FPGA or Tsync driver not running.
- 3. If both time calls fails, the issue could be with the TSync driver, so it's unloaded (and remains unloaded) to allow the Network Processor to continue working. Reloading the Tsync driver requires the unit be rebooted.
- 4. If both calls fail, the oscillator likely glitched, causing both FPGA and KTS to stop responding.
- 5. If **CS_GetTime** fails but **HW_GetTime** passes, FPGA is still working.

D) Normal Entries asserted when just logging into the classic interface browser with versions 5.2.0 and above installed

Aug 3 15:10:57 custservice176 custservice176: [spadmin] ERROR (2) - Error SEC_GetGroup (username[0,1]=quagga) (WEB)

Aug 3 15:10:57 custservice176 custservice176: [spadmin] ERROR (2) - Error SEC_GetGroup (username[1,2]=tcpdump) (WEB)

- These entries are normal log entries when logging into the classic interface web browser with software versions 5.2.0 and above installed (related to tcpdump being added in version 5.2.0)
- Don't need to do anything with tcpdump for these entries to be asserted. They are asserted just by logging into the classic interface browser instead of the newer black/charcoal browser.

E) Associated MySQL System log entries

1. [Log SQLSTATE\[HY000\]: General error: 13 database or disk is full \(WEB\)](#)
 - Indicates Compact Flash (CF) card is full or issue with Lafayette SQLite database file.
 - A. As part of software update failure
 - B. As part of Linux login logs (var/logs directory) being way too large (like 18GB)
 - Refer to Salesforce Case 230530 (Verizon Wireless config saves failing)
2. ["\[WEB\] Log SQLSTATE\[HY000\]: General error: 2006 MySQL server has gone away \(WEB\)"](#)

In summary: update SecureSync software to at least version 5.1.4.

- "General Error 2006" has several causes. Refer to: <http://ronaldbradford.com/blog/sqlstatehy000-general-error-2006-mysql-server-has-gone-away-2013-01-02/>
- Refer to Mantis case 2803 (<http://cvsmantis.int.rolia.com/mantis/view.php?id=2803>)
- Refer to Salesforce cases such as 15337 and 17110
- Indicates the MySQL connection for graph data logging was lost while data was being polled/stored. Only the graphs are affected by this loss of connection.
- In versions prior to 5.1.4, the graphs would just end until the unit was rebooted. Versions 5.1.4 and above, the connection is restored without the need to reboot.

(Email Keith sent to Open Access, 9 Feb 15) Per your inquiry, the "General error: 2006 MySQL server has gone away (WEB)" entry is a very common entry indicating something happened to the SecureSync's MySQL database which is used for the newer web browser functionality (not the earlier "classic interface" browser). There is a broad range of internal possible conditions that can cause this entry to be asserted.

In more recent versions of SecureSync software (versions 5.1.4 and above) this database was made more robust by giving it the capability to repair itself while the SecureSync continues to operate. In earlier versions of software, a reboot of the time server was needed to make repairs to the database, because they could only be made at startup.

Typically, an issue with the MySQL database only affects the web browser. We can't say what errors in the database caused it to need to repair itself, only that with version 5.1.5 software installed, it was able to repair itself without the need to reboot the SecureSync.

Q Question from Keith to Ron regarding above email: Are we still seeing MySQL in our newer versions, such as 5.1.7 or 5.2.0 (I don't recall noticing these entries, but wasn't really concentrating on looking for these messages). If so, are they affecting the operation of the browser or rest of the unit?

A Response from Ron Dries (11 Feb 15)

It depends on when MYSQL "goes away" or repairs itself. The error comes from after the repair occurs a logging task in the system that stores data into MYSQL, primarily for the web UI graphs, can no longer see MYSQL because it has changed. In 5.1.5 a fix was put into place to detect this condition and update the logging task to use the repaired MYSQL. However if the repair occurs after we've checked the condition and started logging the message could still be asserted in the logs. Next time through however the logging task will see what happened and update itself and fix the error.

In software versions prior to 5.1.5 it would stay in this error condition and data that was meant to be stored in the database couldn't get written. In 5.1.5 and later the fix is in place, however there is still a chance a log might get written depending on when MYSQL goes through the repairing process. As for the effect on the system, if the error occurs during a save of data to the MYSQL table that save could be lost but the next time through after the condition has been detected and fixed the data will be resaved. The logging period is such that it will be very difficult to notice any gap in the graphs.

I would like to take a look at the logs if you have them to see how frequently this may be occurring, so when you have them I'll take a look.

Response Keith sent, based on info from Ron- Regarding the periodic MySQL error messages you are observing in the SecureSync logs, I have some additional information for you.

To begin, MySQL is a third-party database that was added in software version 5.1.0 to store the configurations for the newer web browser. We also use it to store the data that is used to generate the oscillator and GPS graphs that are used in the newer browser, such as the GPS SNR/Number Satellites tracked graphs and the DAC value graphs for the oscillator, for examples.

For many reasons unrelated to the SecureSync, the database may need to periodically repair/clean itself up. This may requires the database to restart itself. We are often polling the GPS receiver and oscillator to log this data for the browser graphs to display the data. If the logging connection to the database happens to be lost for any reason after the SecureSync has started sending the its polled data for graphing, the logging transfer connection will be temporarily lost and the log entry you observed is asserted to indicate this. Note the configs use a different connection to the database than the graph data and this entry only applies to the graph data. As the graph data is often being polled and the parameters change very little, a momentary loss of logging connection to the database, even if the data point isn't able to be stored at that particular moment, will not be noticeable in the graphs.

This log entry doesn't have anything to do with the operation of the SecureSync itself (no need to clean, reboot it, etc). The version 5.1.5 update just allows the database logging connection to be restored automatically if the database restarts or if the graph logging connection happens to be lost for any reason. In prior software versions, the unit needed to be rebooted in order to re-establish the logging connection. So if the logging connection happened to be lost in the earlier versions, the graphs in the browser would stop (not show the most recent data because the graph data stopped being able to be stored in the database) until the SecureSync was rebooted. Now a new graph data connection is automatically created, before sending each new graph data to the database, if it was previously lost, with no noticeable effects on the graphs.

We would just like to see how often the logging connection needs to be re-established, by reviewing these particular entries in the System log. Could you send us a log bundle (which includes the System log) from this SecureSync?

All of the SecureSync's logs (including those shown in the browser and also those in the background) can be easily bundled into one file and then exported from the SecureSync to send as an attachment. Instead of copy/pasting all of the log entries into a Word document, starting in Archive software update version 5.1.2, the logs can be easily saved to single bundled file and exported into a networked PC. Earlier versions of software allowed the bundle to be created, but then the file still needed to be transferred out using an FTP/SCP connection. Now, a button in the web browser alleviates the need to create an FTP session to transfer this file out to a PC.

"[system] Updating UTC-GPS Offset value from 0 to 16. (KMOND)": Occurs at each power-up after reading this from the GPS

receiver (expected entry at each power-up)

Note: If this entry is also followed by the following entry: “[system] ntp monitor stopping ntpd, found 15 second difference (NTPMOND)” this is likely due to software issues with the Trimble Res-SMT-GG receiver. See additional info on this further below.

“ERROR (2) - Error SEC_GetGroup (username[0,1]=quagga) (WEB)”

- Refer to Mantis case 2979.
- This is a new log entry starting in update version 5.2.0.
- Note: “Quagga” is a new user account added for “NTP over Anycast” mode
- This message just indicates someone opened the “classic interface” web browser (even if no changes were made in this browser). This message is not asserted when the newer browser is accessed and doesn’t indicate any problems with the time server. This entry is just because the quagga user account doesn’t exist in the “classic interface browser”.

F) System logs associated with KTS (KHTD) (Kramden Host Timing Daemon for input to NTP)

- KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running.

KTS Host Time Daemon has restarted (KHTD):

- This entry indicates NTP was restarted (automatically due to an NTP config change or manually by a user)

KTS Host Time Daemon has terminated (KHTD):

- This entry indicates NTP shutdown for halt/reboot by a user (other daemons will also be terminated, as well).

G) System logs associated with NTP

1. NTPMOND monitor restarting NTP

- NTPMOND “wakes-up” and check NTP every 16 seconds to check if NTP is running and if it’s within 1 second of the System Time (while synced to System Time)
- NTPMOND will restart NTP, if NTP is in sync and the time error from KTS is 1 second or greater, or if NTP exceeded sanity limit of 1000 seconds (16min 40 sec) which can cause it to stop running.

Note: Per Ron Dries, NTPMOND “wakes-up” every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resync and be useable again.

[system] ntp monitor stopping ntpd, found 1 second difference (NTPMOND) followed by:

[system] ntp monitor restarting ntpd (NTPMOND)”

NTP sanity check failed due to <1000 second (16 Min 40 sec) time correction. NTP monitor daemon restarted NTP to apply this correction. System Time was likely manually changed while NTP was still running (input reference may have changed, for instance).

2. NTP step threshold of 128 ms

NTP also has its own Reference time change limits, as well (NTP step threshold- 128ms)

- If NTP's selected input changes by **128 milliseconds or less**, NTP **slews** to the reference
- If NTP's selected input changes by **more than 128 milliseconds** (and this error persists for more than the steptout threshold which has a default value of 900 seconds), NTP **steps** it's time to the reference.

3. SNMP related System log entries

- [spadmin] SNMP agent failed to startup (SNMPAL)
- SNMPSAL tried to restart SNMPAD but was not able to do so. Software should be updated to at least version 5.2.1. Refer to the SNMP troubleshooting section in this doc.

4. System logs associated with Front panel

[system] Front Panel daemon did not detect or initialize the Keypad LCD panel (FPD)
 Note: This entry is only expected if this is a Model 9489 (which has no front panel)

[webui] ERROR (7) - ERROR in KTSAL_Set: GR_SetConstSel 0 0 0 (KTSAL)

- Error condition that can occur in versions 5.1.7 and below when changing the configurations of a Res-SMT-GG receiver that doesn't have the Glonass option enabled. This condition is described in more detail in the "GNSS input" section (just search for "ERROR in KTSAL_Set: GR_SetConstSel" to easily find it).

[web] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'phase_error' cannot be null (WEB) (followed by a series of ktsal failures)

- Observed with version 5.1.7 after changing the System Time while synced with GPS.

Per Oleg, KTS is restarted if a large unexpected time change occurs. The KTS failures were likely due to KTS not being available while KTS was being restarted.

5. Issues related to Trimble RES-SMT-GG GNSS receivers (~Oct 2014)

Note: These System log entries may also be accompanied by related Timing.log entries such as the following:

[system] 2014 224 02:33:38 002 Error: CS_Set(CS_SA_LEAP_SEC) call from GR. (this entry indicates the receiver was trying to erroneously change the leap second offset to some arbitrary value. But a mask we put in place prevented it from being able to be changed)

6. Issue with erratic log entries "no newlines" (no new lines)

"ERROR (7) - ERROR no newlines in response in KTSAL_Get (KTSAL)"

- Applicable in at least version 5.1.4 software.
- Refer to Deviation (ECN) 3481
- Refer to Mantis case 2796 <http://cvsmantis.int.rolia.com/mantis/view.php?id=2796>
- Apparently related to software issues with the Trimble Res-SMT-GG receivers

Email from Dave West (20 May 2014) There are 2 errors that occur in logs regarding the GNSS receivers and the 5.1.4 Release. In the test Procedure, there should be no errors in the system log. With Release 5.1.4, a bug was found randomly sending out the following errors

[webui] ERROR (7) - SPEC_KTSAL_EN=true XO_GetSerialNo 0 (KTSAL)
 [webui] ERROR (7) - ERROR no newlines in response in KTSAL_Get (KTSAL)

[webui] ERROR (7) - SPEC_KTSAL_EN=true XO_GetPhaseError 0 (KTSAL)
[webui] ERROR (7) - ERROR no newlines in response in KTSAL_Get (KTSAL)

These errors are acceptable for shipment per this Deviation:

- A) Leap second incorrectly scheduled:[system] Scheduled Leap Second: +1 sec at 00:00:00 148/2017 UTC (KMOND)
 - B) **UTC offset value changes on its own** [system] Updating UTC-GPS Offset value from 16 to 3. (KMOND) (Note the second value can vary).
- A work-around to prevent this event causing a temporary time error / time jump was added in software version 5.1.5.
-

7. "ERROR in KTSAL" associated entries

- Repeated groupings of several "Failed to read" AND "Failed to get" Error entries asserted in System.log

Example entries that may be asserted:

Failed to read GPS fix data from KTS (GPSD)
ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset.
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read oscillator frequency error from KTS (KAD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)

- Likely due to ETX, or the parts associated with KTS: Micro (U1) 10MHz oscillator FPGA (U40) or EEPROM (U2). FPGA may need to be reloaded at factory.

Per Dave Sohn, KTS crashing not likely due to the memory consumption issue.

Entries indicate KTS crash/ KTS not talking to network processor software. Logs just below are from Salesforce case 15055 (Andy Felde with Drew Wireless. Found it needed a new oscillator)

Similar logs in Salesforce Cases:

15055 (found it needed new oscillator)
11832 (Also reported no SSH. Found bad ETX),
14375 (bad FPGA),
14744 (v5.1.4 software) needed the KTS firmware re-programmed
15326 (Open Access with v4.7A software). John also reported the front panel time display was frozen/locked up and no SSH. Happened more than once a couple weeks apart.

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset.

(KMOND)

[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset.
(KMOND)

[system] Failed to read alarm info from KTS (KAD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)

[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read oscillator frequency error from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current sync state (DISCMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 12:55:43 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)
Jun 23 12:55:47 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
Jun 23 12:55:49 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] ntp monitor stopping ntpd, found 1376668877 second difference (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)

[system] KTS Host Time Daemon has restarted (KHTD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read oscillator frequency error from KTS (KAD)
[system] Failed to get current sync state (DISCMOND)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read oscillator frequency error from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
Jun 23 12:59:12 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get

variable Timescale Offset. (KMOND)

Jun 23 12:59:17 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 12:59:19 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)

Jun 23 12:59:21 Spectracom Spectracom: [system] Failed to get current sync state (DISCMOND)

Jun 23 12:59:28 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 12:59:30 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetLeapSec 0 (KTSAL)

Jun 23 12:59:32 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get Leap Second. (KMOND)

Jun 23 12:59:36 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)

Jun 23 12:59:38 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 12:59:41 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)

Jun 23 12:59:45 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)

Jun 23 12:59:48 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)

Jun 23 12:59:50 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)

Jun 23 12:59:52 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)

[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)

[system] Failed to read GPS antenna status from KTS (GPSD)

[system] Failed to read alarm info from KTS (KAD)

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)

Jun 23 13:00:02 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)

Jun 23 13:00:05 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)

Jun 23 13:00:08 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)

Jun 23 13:00:12 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)

Jun 23 13:00:14 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 13:00:18 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)

Jun 23 13:00:21 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)

Jun 23 13:00:23 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 13:00:27 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)

Jun 23 13:00:29 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 13:00:35 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)

Jun 23 13:00:37 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)

Jun 23 13:00:39 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)

Jun 23 13:00:43 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)

Jun 23 13:00:46 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)

Jun 23 13:00:48 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)

Jun 23 13:00:50 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 13:00:52 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)

Jun 23 13:00:57 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)

Jun 23 13:00:59 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)

Jun 23 13:01:01 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)

Jun 23 13:01:06 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)

Jun 23 13:01:08 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)

Jun 23 13:01:11 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)

Jun 23 13:01:13 Spectracom Spectracom: [system] ntp monitor stopping ntpd, found 1376669162 second difference (NTPMOND)

Jun 23 13:01:15 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)

[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)

Jun 23 13:01:18 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)

Jun 23 13:01:21 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)

Jun 23 13:01:23 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)

Jun 23 13:01:25 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)

Jun 23 13:01:25 Spectracom Spectracom: [system] KTS Host Time Daemon has restarted (KHTD)

Jun 23 13:01:27 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:01:30 Spectracom Spectracom: [system] ntp monitor restarting ntpd (NTPMOND)
Jun 23 13:01:31 Spectracom Spectracom: [system] Failed to get current sync state (DISCMOND)
Jun 23 13:01:33 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
Jun 23 13:01:35 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
Jun 23 13:01:38 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:01:46 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:01:48 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:01:51 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 13:01:53 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
Jun 23 13:01:57 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
Jun 23 13:01:59 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:01 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:02:06 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:09 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:02:12 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:14 Spectracom Spectracom: [kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
Jun 23 13:02:14 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
Jun 23 13:02:16 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:02:18 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
Jun 23 13:02:22 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 13:02:24 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:26 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:02:28 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
Jun 23 13:02:33 Spectracom Spectracom: [kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)
Jun 23 13:02:33 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
Jun 23 13:02:35 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)
Jun 23 13:02:37 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:02:44 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:02:46 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
Jun 23 13:02:48 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:53 Spectracom Spectracom: [kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2 (KTSAL)

Error (4) Error in KTSAL_Get messages

Example entries

[webui] Error (4) Error in KTSAL_Get SPEC_KTSAL_EN=true GPR_GetProfile 0 1 (KTSAL)
[webui] Error (4) Error in KTSAL_Get SPEC_KTSAL_EN=true GPR_GetEthTrans 0 1 (KTSAL)
[webui] Error (4) Error in KTSAL_Get SPEC_KTSAL_EN=true GPR_GetControl 0 1 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetPhaseError 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetCalVal 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GPR_GetUnctMasterProp 0 1 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetPhaseError 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetFreqError 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetPhaseErrorLim 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GPR_GetPortSpeed 0 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetCalVal 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GPR_GetEthTrans 0 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GPR_GetTimeProp 0 1 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetMode 0 (KTSAL)
[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true SS_GetTimeStamp 0 0 0 (KTSAL)

Email from Ron Dries (25 Aug 2020) The screenshot with the **Error 4 KTSAL_Get** messages is just indicating that the web UI tried to query the timing system for status but it was unable to, due to a session log out. We see these errors because the web UI issues a query and then the user is logged out, and the query is unable to finish.

Keith's response to customer: As I alluded to earlier, while a user is logged into the SecureSync's web browser, the web browser pages *such as the GB PTP status page as one quick example) send "queries" (API calls) to a separate software assembly within the SecureSync, referred to as the "KTS Timing System". The KTS software responds back to the queries for the browser to report the data that was requested.

The error messages you inquired about just indicate that the KTS software responded back to the browser with the requested data. But the web browser wasn't able to receive/display the requested information, because the user's browser session had ended/timed-out before the browser could receive/display it. These entries are not unexpected and not any indication of a problem with the SecureSync.

"STR_" error messages in System log (Versions 5.8.0 and above only)

1. "ERROR in KTSAL_Get:SPEC_KTSAL_EN=true STR_GetSubscription 0.0 (KTSAL)"

- Refer to JIRA ticket SSS-505 (completed ~11 Feb 2019)
- Refer to SF case 171405
- Fixed in 5.8.5 update (July 2019)
- Caused by "STL INFO" menu being displayed on front panel (or rotate menus selected) with no 1204-3D/1204-3E STL card installed in the system.
- Version 5.8.0 added the STL Info menu in all units, even if 1204-3D/3E is installed, If the unit is downgraded to below 5.8.0. this STL menu is no longer exists, so the issue no longer occurs
- if STL card isnt installed, the request by the front panel to display STL data causes this entry to be asserted

email from Keith (1 Nov 18) This "GetSubscription" entry is associated with a purchasable feature we now offer for SecureSyncs, called "STL". In case you aren't familiar with it, it's a satellite signal, similar to GPS, but since these satellites are closer to the earth than the GPS constellation, their signals are stronger. There are other benefits to it, as well.

STL is available with an STL receiver Option Card and a subscription to the service. The version 5.8.0 software update added a new front panel LCD display menu which shows the signal strength of this STL signal. The error message just means that someone was scrolling through the various menu screens, which include the STL menu. But without the STL receiver/option being installed, there was no communications available to report the expected value.

This "errant" entry is expected to be no longer reported if the STL menu is selected, or scrolled thru, via a future software update. There should be no operational concerns if this entry is observed! Thanks again for asking about it, just to be sure it didn't indicate a problem!!

2. [webui] ERROR (13) - ERROR in call to KTSAL_GetProgs in KTSAL_Get (KTSAL)

- This entry is just a logging issue
- It's not an indication of a problem with the equipment
- Fixed in the version 5.1C patch and post 5.1.3 update (5.1.4?) which incorporates this patch (PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates)

3. Rinex Server entry each hour “CAGPS ERROR (1): Failed to retrieve data from Rinex server (CAGPSD)”

- Applicable to version 5.1.3 software only
- Due to A-GPS still running, even though its disabled. Seen only on units on a closed network with no Internet access.
- Refer to knowledge base article 1275 (<https://na8.salesforce.com/ka3C0000000TT7D>).
- Fix is to install version 5.1C patch (PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates
- Logging issue only. Does not adversely affect operation of SecureSync.

4. GPS Monitor daemon starting and terminating from time of power-up

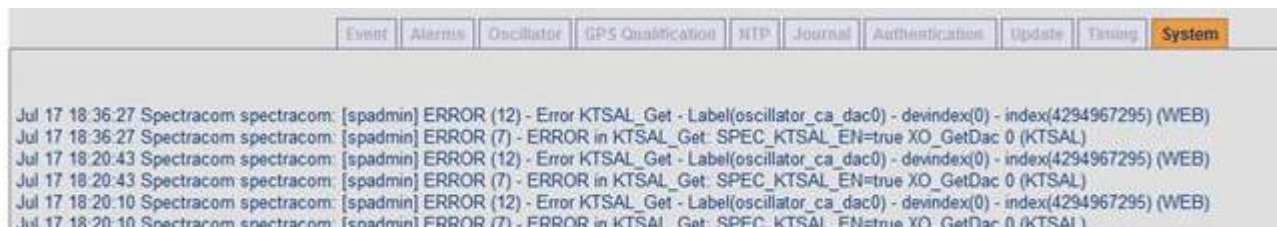
- Refer to Mantis case 2391 and NC7252 for this issue
- Started in version 5.0.0 (in at least versions 5.0.0, 5.0.1 and 5.0.2)
- This is just a logging issue.
- Fix already done for inclusion in the next planned release (version 5.1.0).

5. Issue with erratic log entries in units with Rb oscillator installed

- Refer to Mantis Case 1729.
- Applicable in at least version 4.8.6 software.
- Was fixed in the v4.8.7 update.

Q. I'm getting an error message in the System Log of a 1200-033 Rb. unit I just updated to 4.8.6. This occurs after I select the STATUS/TIME AND FREQUENCY (It is not happening on an OCXO unit)

```
Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
```



A Email from Dave Sohn (6/20/12) There isn't any issue with the unit. This is just a reporting bug. The system is in the background querying the DAC value for some reporting, but that isn't a valid call for a Rubidium unit, so there is an error. There is no effect on operation, and that error doesn't mean there is any problem with the unit. You can enter a Mantis case for it, and we will discuss it in SW CCB.

(8/31/12 KW) Update – the fix for this issue should be in the version 4.8.7 release

Error entry periodically being asserted “[system] ERROR - KW_HR_SetTime returned [rc = 3]”

- Refer to Salesforce cases 14919 (Dongjin) and 12869 (Open Access, Australia)
- Apparently asserted when NTP input tries to set the KTS time but is not able to
- Verify the proper configuration of the NTP Peers and NTP Servers tabs.
- Dongjin had the Enable Stratum 0 PPS reference enabled with a peer configured.

24 June 2014 KW- Per Oleg, this entry indicates KTHD tried to sync NTP from System Time (using the Spectracom driver) but for some reason, KTHD (not NTP) rejected the time. KHTD tries to sync NTP every 16 seconds. This entry indicates that for this one particular instance, KHTD was not able to sync NTP.

Since it couldn't sync NTP on this particular instance (for whatever reason), there was no detrimental effect in any way to the timing performance of the SecureSync at that time.

Internal info only- One thought is our driver may be trying to set the NTP time twice in the same second and only one of the two can be successful???

Patch 4.8S/v5.1.2 and above work-around to Gb dropped packets issue

Note: Refer also to the **much more recent E1000E driver update** made available for Morgan Stanley (“**UpdateGB3421**”): [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Morgan Stanley-5.8.4 NTP performance \(updateGB3421.tar.gz\)](..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Specials\software patches\Morgan Stanley-5.8.4 NTP performance (updateGB3421.tar.gz))

- Refer to the “**1204-06**” section of the SecureSync Option Card document for additional info on dropped packets/RNBC counters

Patch version 4.8S, as well as 5.x.x updates contain a patch to reset the network processor if it stops responding. It checks each of the processors every 10 seconds and resets any of them that stops responding to packets.

Per Dave Sohn- “The port appears to recover within a second or two”. The total time that a port may not respond to packets is the 10 seconds between checks of the processor plus just a couple of seconds for the port to be restarted.

Example entries in the **System** log when the network processor is restarted:

Note this entry indicates which Ethernet port was restarted (“eth1” in this example)

Aug 6 12:34:41 Spectracom Spectracom: [system] GbE port eth1 event: RNBC=51 (KMOND)

Aug 6 13:31:33 Spectracom Spectracom: [system] GbE port eth1 event: RNBC=102 (KMOND)

Timekeeper.log entries

- Timekeeper log added to the log bundles starting in update version 5.2.0
- Placed in the /var/log directory
- Refer to the “**Logs tab**” Section of [VelaSyncAndGeoCustAssist.pdf](#) for details on analyzing logs

Timing log entries

IRIG input troubleshooting

A) SecureSync not syncing to an IRIG source

How to verify IRIG input signal issues

- Example timing.log entries if IRIG input is intermittent

```
Jun 22 15:01:40 Spectracom Spectracom: [system] 2015 173 15:01:39 021 IR irg0 Comm Lost.
Jun 22 15:01:44 Spectracom Spectracom: [system] 2015 173 15:01:44 000 IR irg0 Comm OK.
Jul 2 00:12:43 Spectracom Spectracom: [system] 2000 001 00:00:05 000 IR irg0 Comm OK.
Jul 8 16:53:02 Spectracom Spectracom: [system] 2015 189 16:53:02 021 IR irg0 Comm Lost.
Jul 8 17:06:52 Spectracom Spectracom: [system] 2015 189 17:06:52 000 IR irg0 Comm OK.
Jul 8 17:08:30 Spectracom Spectracom: [system] 2015 189 17:08:30 021 IR irg0 Comm Lost.
Jul 8 17:08:59 Spectracom Spectracom: [system] 2015 189 17:08:59 000 IR irg0 Comm OK.
Jul 8 17:09:23 Spectracom Spectracom: [system] 2015 189 17:09:23 021 IR irg0 Comm Lost.
Jul 8 17:10:28 Spectracom Spectracom: [system] 2015 189 17:10:28 000 IR irg0 Comm OK.
Jul 8 17:20:14 Spectracom Spectracom: [system] 2015 189 17:20:14 021 IR irg0 Comm Lost.
Jul 8 17:20:31 Spectracom Spectracom: [system] 2015 189 17:20:31 000 IR irg0 Comm OK.
Jul 8 17:21:31 Spectracom Spectracom: [system] 2015 189 17:21:31 021 IR irg0 Comm Lost.
```

Timing log entries associated with a uBlox M8T GNSS receiver installed

“ublox GNSS receiver data” reported in Timing log (refer also to “Ublox” section in: [!:\Customer Service\1- Cust Assist documents\Customerserviceassistance.pdf](file:///C:/Customer%20Service/1-Cust%20Assist%20documents/Customerserviceassistance.pdf))

Fields/values

PPS SYNC= x (0= PPS not in sync) (1= PPS is in sync)

H=x (0= Time not in sync) (1= Time is in sync)

Mode=x (0= Single Satellite mode) (1= Standard/Stationary mode) (2= Mobile/Continuous mode)

Note: VersaSync’s factory default mode is **Mobile** mode

tAcc=x (where “x” is Time Accuracy Estimate– reported in nanoseconds)

tAccClk= x (where “x” is Time Accuracy Estimate– reported in nanoseconds???)

indoor= 0 (I believe this indicates the “indoor messaging service” -IMES- being disabled in the ublox receiver)

Note: “IMES” (associated with Japan’s QZSS) appears to be a mode of operation for indoor positioning using low power transmitters

GPS Fix:

None (GPS survey has not yet been completed)

TIMEONLY (5) (GPS survey has completed)

3D (3) (3D fix- with four or more satellites being tracked?)

```
Oct 5 13:18:11 2017 278 13:18:11 000 PPS SYNC=0 H=1 Mode=1 tAcc=2 tAccClk=6 indoor=0 GPS Fix: NONE (0)
Oct 5 13:18:30 2017 278 13:18:30 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Oct 5 13:18:30 2017 278 13:18:30 000 PPS SYNC=1 H=1 Mode=1 tAcc=14 tAccClk=44 indoor=0 GPS Fix: TIMEONLY (5)
Oct 5 13:18:33 2017 278 13:18:33 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Oct 5 13:18:33 2017 278 13:18:33 000 PPS SYNC=0 H=1 Mode=1 tAcc=13 tAccClk=16 indoor=0 GPS Fix: NONE (0)
Oct 5 13:18:34 2017 278 13:18:34 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Oct 5 13:18:34 2017 278 13:18:34 000 PPS SYNC=1 H=1 Mode=1 tAcc=12 tAccClk=13 indoor=0 GPS Fix: TIMEONLY(5)
Oct 5 13:43:10 2000 001 00:00:05 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Oct 5 13:43:10 2000 001 00:00:05 000 PPS SYNC=0 H=1 Mode=1 tAcc=4556 tAccClk=3 indoor=0 GPS Fix: NONE (0)
Oct 5 13:43:10 2000 001 00:00:05 000 GNSS Source of UTC-GPS Offset from Unknown(255) to GPS(2) V=3
Oct 5 13:43:10 2000 001 00:00:05 000 Changing GNSS Source of Leap Second from None(0) to GPS(2) V=3
Oct 5 13:43:10 2000 001 00:00:05 038 GR antenna fault.
Oct 5 13:43:10 2000 001 00:00:06 000 GNSS FIX CHANGE: NONE (0) to 3D (3)
Oct 5 13:43:10 2000 001 00:00:06 000 GR antenna ok.
Oct 5 13:43:10 2000 001 00:00:08 000 PPS SYNC=1 H=1 Mode=1 tAcc=30 tAccClk=56 indoor=0 GPS Fix: 3D (3)
```

Oct 5 13:43:10 2017 278 13:43:03 000 GNSS FIX CHANGE: 3D (3) to NONE (0)
 Oct 5 13:43:10 2017 278 13:43:03 000 PPS SYNC=0 H=1 Mode=1 tAcc=2555 tAccClk=4 indoor=0 GPS Fix: NONE (0)
 Oct 5 13:43:10 2017 278 13:43:03 038 GR antenna fault.
 Oct 5 13:43:10 2017 278 13:43:03 000 GR antenna ok.
 Oct 5 13:43:10 2017 278 13:43:04 000 GNSS FIX CHANGE: NONE (0) to 3D (3)
 Oct 5 13:43:10 2017 278 13:43:04 000 PPS SYNC=1 H=1 Mode=1 tAcc=420 tAccClk=36 indoor=0 GPS Fix: 3D (3)
 Oct 5 13:43:10 2017 278 13:43:05 000 PPS SYNC=0 H=1 Mode=1 tAcc=118 tAccClk=420 indoor=0 GPS Fix: 3D (3)
 Oct 5 13:43:10 2017 278 13:43:06 000 PPS SYNC=1 H=1 Mode=1 tAcc=67 tAccClk=118 indoor=0 GPS Fix: 3D (3)
 Oct 5 13:47:44 2017 278 13:47:44 000 GNSS FIX CHANGE: 3D (3) to NONE (0)
 Oct 5 13:47:44 2017 278 13:47:44 000 PPS SYNC=0 H=1 Mode=1 tAcc=4 tAccClk=4 indoor=0 GPS Fix: NONE (0)
 Oct 5 13:48:04 2017 278 13:48:04 000 GNSS FIX CHANGE: NONE (0) to 3D (3)
 Oct 5 13:48:04 2017 278 13:48:04 000 PPS SYNC=1 H=1 Mode=1 tAcc=165 tAccClk=49 indoor=0 GPS Fix: 3D (3)
 Oct 5 14:15:31 2017 278 14:15:31 000 GNSS FIX CHANGE: 3D (3) to TIMEONLY (5)
 Oct 5 14:15:31 2017 278 14:15:31 000 Standard Survey completed in 2000 sec with 3D-Variance 877643 mm^2
 Oct 5 15:20:33 2017 278 15:20:32 000 Empty UBX FIFO
 Oct 5 15:26:25 2017 278 15:26:25 000 Empty UBX FIFO
 Oct 8 02:41:02 2017 281 02:41:02 000 PPS SYNC=0 H=0 Mode=1 tAcc=3 tAccClk=3 indoor=0 GPS Fix: TIMEONLY (5)
 Oct 8 02:42:06 2017 281 02:42:06 000 PPS SYNC=1 H=1 Mode=1 tAcc=2 tAccClk=2 indoor=0 GPS Fix: TIMEONLY (5)

****Toggling between “GNSS FIX CHANGE: (5) to NONE (0)” / “GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)”**

- Appears to be related to the uBlox receiver either dropping to less than 4 sats, or falling to 0 sats.
- **Suggestion to fix:** try deleting the receiver position for it to perform a new GPS survey.

I 30 01:45:28 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:28 000 PPS SYNC=0 Mode=1 tAcc=19 tAccClk=46 indoor=0 GPS Fix: NONE (0)
 Jul 30 01:45:38 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:38 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
 Jul 30 01:45:38 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:38 000 PPS SYNC=1 Mode=1 tAcc=109 tAccClk=56 indoor=0 GPS Fix: TIMEONLY (5)
 Jul 30 01:45:39 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:39 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
 Jul 30 01:45:39 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:39 000 PPS SYNC=0 Mode=1 tAcc=67 tAccClk=109 indoor=0 GPS Fix: NONE (0)
 Jul 30 01:45:41 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:41 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
 Jul 30 01:45:41 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:41 000 PPS SYNC=1 Mode=1 tAcc=150 tAccClk=75 indoor=0 GPS Fix: TIMEONLY (5)
 Jul 30 01:45:47 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:47 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
 Jul 30 01:45:47 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:47 000 PPS SYNC=0 Mode=1 tAcc=47 tAccClk=75 indoor=0 GPS Fix: NONE (0)
 Jul 30 01:45:50 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:50 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
 Jul 30 01:45:50 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:50 000 PPS SYNC=1 Mode=1 tAcc=85 tAccClk=52 indoor=0 GPS Fix: TIMEONLY (5)
 Jul 30 01:45:54 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:54 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
 Jul 30 01:45:54 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:54 000 PPS SYNC=0 Mode=1 tAcc=43 tAccClk=111 indoor=0 GPS Fix: NONE (0)
 Jul 30 01:46:05 cx01pdix04 cx01pdix04: [system] 2017 211 01:46:05 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
 Jul 30 01:46:05 cx01pdix04 cx01pdix04: [system] 2017 211 01:46:05 000 PPS SYNC=1 Mode=1 tAcc=186 tAccClk=128 indoor=0 GPS Fix: TIMEONLY (5)
 Jul 30 01:54:13 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:13 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
 Jul 30 01:54:13 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:13 000 PPS SYNC=0 Mode=1 tAcc=10 tAccClk=49 indoor=0 GPS Fix: NONE (0)
 Jul 30 01:54:14 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:14 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
 Jul 30 01:54:14 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:14 000 PPS SYNC=1 Mode=1 tAcc=36 tAccClk=10 indoor=0 GPS Fix: TIMEONLY (5)

Timing log entries associated with a STL receiver Option Card installed

- The Timing log now contains burst information. Example log entries below

```
Oct 4 07:32:27 Spectracom Spectracom: [system] 2017 277 07:32:36 000 STL Status: Total Burst:1 Strong Burst:0
Oct 4 07:32:32 Spectracom Spectracom: [system] 2017 277 07:32:41 000 STL Status: Total Burst:2 Strong Burst:0
Oct 4 07:33:17 Spectracom Spectracom: [system] 2017 277 07:33:26 000 STL Status: Total Burst:3 Strong Burst:0
Oct 4 07:33:27 Spectracom Spectracom: [system] 2017 277 07:33:36 000 STL Status: Total Burst:2 Strong Burst:0
Oct 4 07:33:32 Spectracom Spectracom: [system] 2017 277 07:33:41 000 STL Status: Total Burst:1 Strong Burst:0
```

Note: RyanJohnson indicated these entries show marginal reception

SAASM receiver-related entries (not applicable to commercial receivers)

Note: all SAASM log entries below are from the same SecureSync which had low GPS signal strength/nearby jamming (examples of log entries- its not a complete log snippet)

Error 11

- Applicable to SAASM receiver only (Sent directly from the SAASM receiver and not one of our logs)
- Indicates the receiver's BIOS battery is starting to fail, has failed or is not in the circuit (I believe, but not certain, this entry can indicate the on/off switch on the metal plate is off –the factory default position for this switch).

GPS Warning (63): Jamming detected single frequency

- Applicable to SAASM receiver only (Sent directly from the SAASM receiver and not one of our logs)
- Indicates either L1 or L2 is being jammed or has low signal strengths

```
2016 146 00:00:03 000 Current Status (SAASM): Days with keys=39
2016 146 00:00:08 000 SAAS Status Word 1 Changed: 0x80A7
2016 146 00:00:08 000 Days CVd's Available: 39
```

```
May 9 11:38:33 Spectracom Spectracom: [system] 2016 130 11:38:33 000 GPS Warning (62): Can't Acq/Track possible
masking
May 9 11:47:00 Spectracom Spectracom: [system] 2016 130 11:47:00 000 Exit Sync: NumSats=3 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May 9 12:46:33 Spectracom Spectracom: [system] 2016 130 12:46:33 000 >=4 Measures
May 9 12:46:33 Spectracom Spectracom: [system] 2016 130 12:46:33 000 Tracking >=4 SV in State 5
May 9 12:46:34 Spectracom Spectracom: [system] 2016 130 12:46:33 000 Enter Sync: NumSats=4 NavConv=1 FOM=1
TFOM=3 HERR<=8 m VERR<=10 m mode=2 user=2
May 9 12:47:04 Spectracom Spectracom: [system] 2016 130 12:47:04 000 State 3 Operation (1)
May 9 12:47:08 Spectracom Spectracom: [system] 2016 130 12:47:08 000 Exit Sync: NumSats=3 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May 9 12:47:10 Spectracom Spectracom: [system] 2016 130 12:47:10 000 State 3 Operation (0)
May 9 12:47:10 Spectracom Spectracom: [system] 2016 130 12:47:10 000 Enter Sync: NumSats=4 NavConv=1 FOM=1
TFOM=3 HERR<=8 m VERR<=10 m mode=2 user=2
May 9 12:47:21 Spectracom Spectracom: [system] 2016 130 12:47:21 000 <4 Measures
May 9 12:47:24 Spectracom Spectracom: [system] 2016 130 12:47:24 000 Exit Sync: NumSats=3 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May 9 16:07:34 Spectracom Spectracom: [system] 2016 130 16:07:34 000 Tracking >=4 SV in State 5
May 9 16:17:57 Spectracom Spectracom: [system] 2016 130 16:17:57 000 GPS Warning (51): RAIM exclusion failed
May 9 16:18:27 Spectracom Spectracom: [system] 2016 130 16:18:27 000 GPS Warning (51): RAIM exclusion failed
May 9 16:18:57 Spectracom Spectracom: [system] 2016 130 16:18:57 000 GPS Warning (51): RAIM exclusion
May 9 17:59:21 Spectracom Spectracom: [system] 2016 130 17:59:20 000 GPS Warning (51): RAIM exclusion failed
May 9 18:00:04 Spectracom Spectracom: [system] 2016 130 18:00:03 000 Exit Sync: NumSats=7 NavConv=1 FOM=1 TFOM=4
HERR<=8 m VERR<=9 m mode=2 user=2
May 9 18:00:21 Spectracom Spectracom: [system] 2016 130 18:00:20 000 Enter Sync: NumSats=7 NavConv=1 FOM=1
TFOM=3 HERR<=8 m VERR<=9 m mode=2 user=2
May 9 18:07:28 Spectracom Spectracom: [system] 2016 130 18:07:27 000 GPS Warning (51): RAIM exclusion failed
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:01 000 GR entered failure state.
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:10 000 GSSIP: Communication OK.
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:11 000 GR exited failure state.
```

May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:14 000 RCVR passed self-test
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:15 000 Current Status (SAASM): Days with keys=27
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:15 000 Current Status (SAASM) Changed: 0x0002
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:15 000 Current Status (SAASM): Contains today's key
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 000 SAASM EVENT: KEYS_VALID=TRUE The SAASM Key Is Valid
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 005 GR entered failure state.
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 000 GR exited failure state.
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 000 GR antenna ok.
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:18 000 >=4 Measures
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:18 000 Tracking >=4 SV in State 5
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:20 000 NAV Data Valid
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:21 000 Enter Sync: NumSats=8 NavConv=1 FOM=1 TFOM=3 HERR<=13 m VERR<=19 m mode=0 user=0
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAAS Status Word 1 Changed: 0x809B
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 Days CVd's Available: 27
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 RCVR is keyed
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAAS Status Word 2 Changed: 0x04A0
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 KDP IP Zeroize Not Attempted
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 KDP CV Zeroize Not Attempted
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 KDP Status: Operational
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAASM Lock Status: RCVR Locked
May 9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAASM Memory Status: Not Zeroized
May 9 18:55:36 Spectracom Spectracom: [system] 2016 130 18:54:45 000 GPS Warning (63): Jamming detected single frequency
May 9 18:55:36 Spectracom Spectracom: [system] 2016 130 18:55:35 000 GPS Mode changed from Continuous [0] to Averaging [2].
May 9 18:55:39 Spectracom Spectracom: [system] 2016 130 18:55:39 001 HR: Enabling Host Disciplining Mode.
May 9 19:05:10 Spectracom Spectracom: [system] 2016 130 19:05:10 000 GPS Warning (63): Jamming detected single frequency
May 9 19:14:28 Spectracom Spectracom: [system] 2016 130 19:14:28 000 Current Status (SAASM): Days with keys=55
May 9 19:14:29 Spectracom Spectracom: [system] 2016 130 19:14:29 000 SAAS Status Word 1 Changed: 0x80B7
May 9 19:14:29 Spectracom Spectracom: [system] 2016 130 19:14:29 000 Days CVd's Available: 55
May 9 19:15:18 Spectracom Spectracom: [system] 2016 130 19:15:18 000 GPS Warning (63): Jamming detected single frequency

Harris software only (such as version 5.4A)

Phase Chg(1): Fph=108.3551 LAvg=95.2027 Thr=200.0000

- This entry is at least currently limited to just Harris update version 5.4a only

Per Paul Myers (20 Jun 16) This is a log entry for the new Harris feature to detect 1PPS Jumps from the receiver. It detected a phase change.

GR: Enter Holdover due to Phase Invalid Timeout.

- Refer to Salesforce case 25697

“Error: CS_Set(CS_SA_LEAP_SEC) call from GR”

- This condition is caused by firmware issues with the Trimble RES-SMT-GG receiver (firmware version 1.07 which was made available starting in software update version 5.1.7)

Per Dave Sohn (21 Oct 2014) We're not sure yet whether 1.07 fixes this specific issue. We received conflicting info from Trimble. However, this error does not cause any bad side effects so can be ignored by the customer and will be resolved in an upcoming SW release.

“GR antenna fault” / “GR antenna ok”

- These entries indicate opens/shorts being detected in the antenna cable and then clearing.

“GPS Startup/Reset detected”

- There are three (3) primary reasons for this alarm and condition to occur:
 - 1) System reboot
 - 2) Receiver configuration changes that require receiver to reset (such as changing the receiver mode from Standard to mobile mode). Detailed in “A)” further below
 - 3) Marginal/poor reception. Detailed in “B)” further below.

Note: Paul Myers believes the receiver reset due to marginal reception is likely associated with factors such as multipath reception causing the receiver to perform another GPS survey to recalculate its position. This will affect its 1PPS output.

“2000 001 00:00:01” after [system] (default boot-up year and time)

[system] 2000 001 00:00:01 000 GPS Startup/Reset detected

- SecureSync was rebooted or power cycled
- Default startup date and time: Year 2000 and time of 00:00:00 (Date and time is then updated by RTC to the estimated correct date/time).

2014 134 01:28:54 000 GPS Startup/Reset detected (Correct year/date after [system])”

[system] 2014 328 15:50:58 000 GPS Startup/Reset detected

- **Likely causes are either:**

- User made config changes to the receiver that required the receiver to need to restart

Note: Look in the Journal log to see if there are any corresponding log entries for GPS/GNSS receiver config changes being made. Example change that will reset the receiver include changing the receiver mode – such as standard to mobile mode for instance).

- RES-T GPS receiver reset itself in an attempt to improve marginal reception.

- The fix to prevent this from occurring is to: either improve GPS reception or upgrade to Glonass Option.

Modified Email Keith sent to Logix (2 June 2014)

Regarding the “GPS receiver resets” and associated SecureSync alarms, the GPS receiver may internally reset itself when operating in a marginal reception environment (such as tracking only 2 or 3 satellites, for example). This is an attempt to improve its reception. The other condition that causes the GPS receiver to reset is when the unit first boots-up. The way to differentiate between the two conditions is in the associated log entry for each, the year will be “2000” when its due to a reboot, or the year will be the current year when the receiver resets due to marginal GPS reception. Below are examples of each type of receiver reset.

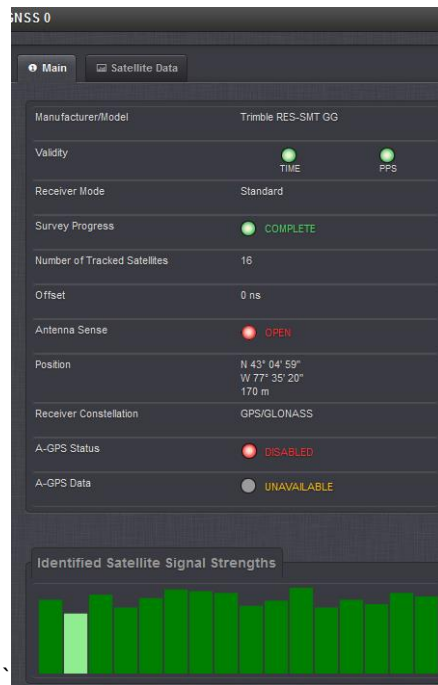
Feb 21 19:31:06 Spectracom Spectracom: [system] 2000 001 00:00:01 000 GPS Startup/Reset detected
Feb 21 19:31:06 Spectracom Spectracom: [system] 2000 001 00:00:01 000 GPS Startup/Reset detected
Feb 21 19:31:06 Spectracom Spectracom: [system] 2000 001 00:00:03 000 GPS Startup/Reset detected
Feb 21 19:31:07 Spectracom Spectracom: [system] 2000 001 00:00:03 000 GR antenna ok.
Mar 7 05:48:01 HOU-GPS-02 HOU-GPS-02: [system] 2014 066 05:48:00 000 GPS Startup/Reset detected
Apr 9 22:38:12 HOU-GPS-02 HOU-GPS-02: [system] 2000 001 00:00:01 000 GPS Startup/Reset detected
Apr 9 22:38:12 HOU-GPS-02 HOU-GPS-02: [system] 2000 001 00:00:02 000 GPS Startup/Reset detected
Apr 9 22:38:12 HOU-GPS-02 HOU-GPS-02: [system] 2000 001 00:00:03 000 GPS Startup/Reset detected
May 13 01:32:36 HOU-GPS-02 HOU-GPS-02: [system] 2014 133 01:32:36 000 GPS Startup/Reset detected

When the GPS receiver resets because of marginal or poor GPS reception, its 1PPS output will likely be restored out of phase with where it was at before it was reset. While the receiver is resetting, it will track 0 satellites for a few seconds as the logs you sent were indicating). Also, the Frequency alarm will be asserted because of the loss of 1PPS input (or if GPS goes not valid for a period of time). Once the internal oscillator has been re-disciplined, the Frequency alarm will clear. The Restart Tracking you had performed is a way to expedite clearing of this alarm.

To prevent the receiver from being reset due to marginal reception, the receiver needs to be able to track more satellites on a regular basis. There are essentially two ways to increase the number of satellites it can track (one may be more feasible than the other). The first it to relocate the GPS antenna to an area with more view of the sky (such as on top of the parking garage, instead of on the side

of the building). However, if this isn't possible, the other method is to use the Model 8230 GNSS antenna (instead of the earlier Model 8226 GPS antenna) and a GNSS receiver inside the SecureSync, with the Glonass satellite Option enabled. This will allow the newer Model receiver to track both GPS and Glonass satellites simultaneously. Instead of tracking just 2 GPS satellites, it's likely to also track a few Glonass satellites also. So to the receiver, it's now tracking 5 satellites instead of 2 satellites, for example. It goes from poor reception to good reception with no need for it to try to improve the reception it has. This is the primary advantage of the Glonass satellite capability recently becoming available for SecureSync.

With Model 8230 GNSS antennas already installed, instead of the earlier Model 8225 antenna), in order to enable the Glonass capability, the two SecureSyncs would just need to be returned for a receiver replacement/Glonass enabling (unless they already have the newer GNSS receiver installed –then the option can be enabled in the field). If the top of the **Interfaces** -> **GNSS 0** page of the browser reports the receiver Model is a Resolution T receiver, this is a GPS only receiver and needs to be replaced for Glonass capability. The newer GPS/Glonass receiver is a Model RES-SMT receiver (as shown below):



As a quick summary of the Glonass satellite capability, this particular RES-SMT receiver is tracking satellites, seven of which are Glonass satellites.

Please let us know if you would like additional information on upgrading the SecureSyncs to Glonass capability to improve the number of satellites each of the SecureSyncs can track.

“Rb peak voltage error(val=0, min=51, max=255)” entries.

- The oscillator is reporting to the SecureSync that it isn't operating normally. This value inside the oscillator is reading “0” when it should be between 51 and 255.

Email from Mark McGregor (20 Aug 2014) When that signal is low there is no atomic lock and the 10 MHz will be off frequency. I would suggest the customer measure the 10 MHz. When the Rb peak signal is too low it will either be stuck 100 to 200HZ low or will move below and above 10 MHz trying to find the Rb peak signal. If the 10 MHz looks OK, then the failure is intermittent. The SecureSync does a great job of monitoring the Rb health. It reads health information every second, so if the atomic clock is lost even for a moment, it will report it right away in the logs. There are many case of this intermittent failure in other RMA and factory production test.

Transfer.log (transfer log entries)

- Entries related to software updates, for the save and restore of the configs.
- This log is not viewable via the browser (its included in the saved log bundle)
- This log is not wiped when performing a “clear all logs” in the browser

Update.log (update log entries)

- Normal Log entries from our SecureSync 10.2.100.176 after successful update of 5.1.5 to 5.1.6 (ascending order)

```
Oct 20 11:48:43 Custservice Custservice.176: [sw-upgrade] Using installed update tool from current version (SWUAL)
Oct 20 11:52:25 Custservice Custservice.176: [sw-upgrade] Using update tool supplied by upgrade (SWUAL)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Application 5.1.5 5.1.6 Upgrade Needed (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Licensing - No Upgrade Available (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Licensing - No Upgrade Available (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Timing FW 3.17 3.17 No Upgrade Needed (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Timing FPGA 3.17 3.17 No Upgrade Needed (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] GNSS 1.6 - No Upgrade Available (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] Timing EEPROM 1.00 No Upgrade Available (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] OC 1 ID 1F 0101 1.01 No Upgrade Needed (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] OC 2 ID 06 0000 - No Upgrade Available (SWUE)
Oct 20 11:53:43 Custservice Custservice.176: [spupdate] OC 3 ID FF 0000 - No Upgrade Available (SWUE)
Oct 20 11:53:43 Custservice Custservice.176: [spupdate] OC 4 ID FF 0000 - No Upgrade Available (SWUE)
Oct 20 11:53:43 Custservice Custservice.176: [spupdate] OC 5 ID 01 0103 1.03 No Upgrade Needed (SWUE)
Oct 20 11:53:44 Custservice Custservice.176: [spupdate] OC 6 ID 32 0121 1.21 No Upgrade Needed (SWUE)
Oct 20 11:53:44 Custservice Custservice.176: [spupdate] Preparing Application Software for Upgrade (SWUE)
Oct 20 11:53:54 Custservice Custservice.176: [sw-upgrade] Upgrade Initiated, Reboot Required: /home/spectracom/update516.tar.gz (SWUAL)
Oct 20 11:59:33 TRANSFER_ENGINE: [SUCCESS] Update successful
```

Update log entries when an issue occurred with an update

A) Update log contains only the first entry “Using installed update tool from current version (SWUAL)”

- Indicates the CF card was likely too full to unpack bundle. Be sure to delete any previous version bundles. Perform a **df -h** command to check disk usage.

```
spadmin@Spectracom ~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M  53% /
/dev/hda1       963M  480M  434M  53% /
devtmpfs        248M    0  248M   0% /dev
```

B) Update log entry indicates “[sw-upgrade] Upgrade Initiated, Reboot Required: home/spectracom/update517.tar.gz (SWUA)”

- Observed with 5.1.4 to 5.1.7 update
- Should be fixed with 5.1.J beta/ Version 5.2.0 software update (Feb 2015).
- Refer to Salesforce cases such as 16749 (Jump Trading)
- Unit doesn’t complete the upgrade because it can’t reboot.
- Reboot commands via browser/CLI don’t work.
- Requires a hard power cycle of the unit to finish the update.
- Dave Sohn noted this has been observed with Verizon likely due to the potential pipe software command issue in 5.1.7 and below. “This sounds similar to the Verizon issue as well. I believe when we had an issue with one of the units, the hung process prevented the reboot. In that case, it took a hard power cycle to recover it.”

“Upgrading GNSS Firmware (SWUE)” followed by “Problem writing GPS FW image (SWUE)”

- Starting software version (before update process was started) was versions 5.1.4 or below. The RES-SMT-GG receiver’s firmware wasn’t able to be updated because the starting version needs to be version 5.1.5 or higher to be able to update the receiver.
- Run the same software update process again to successfully update the GNSS receiver’s firmware.

Version is not found” entry following “Restoring Config backup” entry when performing a “config restore”

Id	Date	Entity	Message
8	Oct 22 20:22:29	bundle	version is not found
7	Oct 22 20:21:44	bundle	version is not found
6	Oct 22 20:20:42	[webui]	Restoring config backup /home/spectracom/xfer/config/seuresync.conf (SWUAL)
5	Oct 22 15:43:41	bundle	version is not found

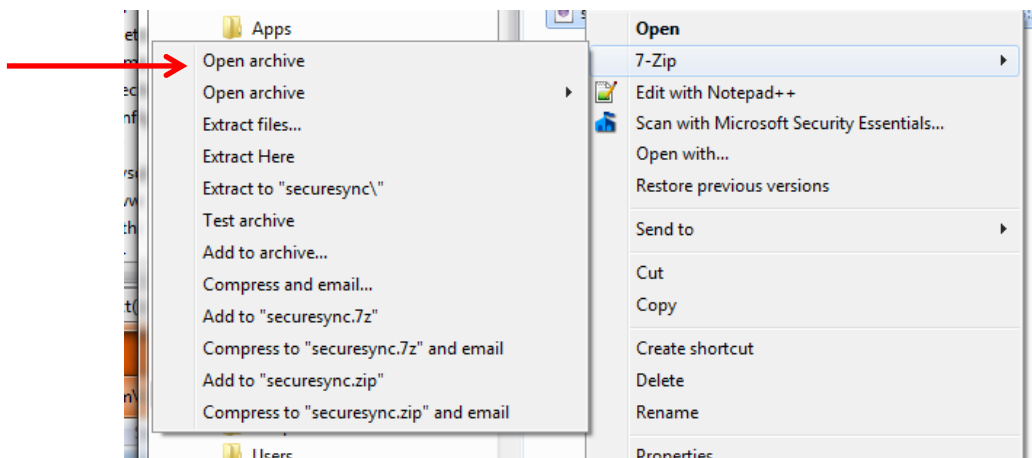
- Has been observed with a corrupt config backup file.

Note: Trying to apply a saved config file saved from a newer version than the target unit may result in a “**Version is not found**” entry in the Update log.

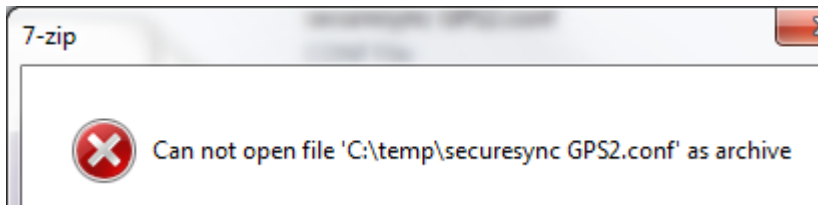
Important Note: When manually transferring the config file using FTP/SFTP, make sure to **BINARY** mode (not ASCII) ASCII mode will corrupt the file.

There is only one way to confirm if the config backup file has been corrupted.

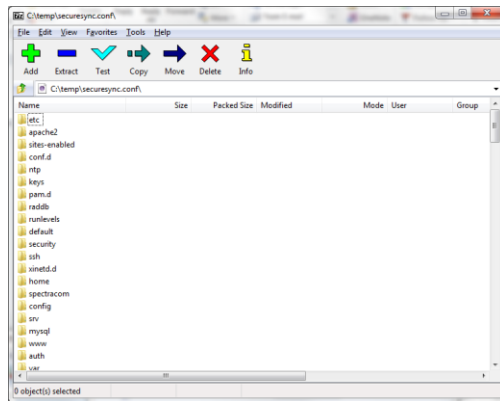
- 1) Save config backup to “temp” directory for instance
- 2) Right click and select a program to extract the file (such as 7-Zip)
- 3) Select “Open Archive”



- 4) Below is an example report of a **corrupt file**.



Example of a valid config backup file (Open Archive)



- This may happen when trying to apply to a target unit (with 5.0.0 or higher software) a backup file that was taken from a later version of software, which was also 5.0.0 or above (5.1.5 backup was trying to be restored to a version 5.1.4 SecureSync. But a newer version can't be installed on an earlier version, even if both are 5.0.0 and above with an MOTD file). But this isn't confirmed.
- This may also occur when trying to restore configs from a v4.8.9 or below unit to one running 5.0.2 or above. But this isn't confirmed.

Email Keith sent (22 Oct 14) Thanks for your email and for reporting what you are observing!

It looks like you are likely trying to apply a saved config from versions 4.8.9 or below to a newer version of 5.1.2 or greater. Please be aware that due to significant config changes, earlier saved config files can't be applied to these much newer versions of software.

Attached for your reference is a document that discusses how to backup and restore configs. Please refer to the note at the bottom of page 1 that discusses this limitation in more detail.

However, if the config save was performed on a SecureSync with software versions 5.x.x software installed, please let me know and we can go from there!

user.log entries

- This log is not accessible from the browser. Is in the Saved Logs bundle.
- This log is not wiped when performing a “clear all logs” in the browser
- Refer to the LDAP/Radius section of this document for more info on the User log entries.

System Reboot or halt (not power cycle)

“shutting down for system reboot”

pam_radius_auth: RADIUS server 10.82.122.16 failed to respond
pam_radius_auth: All RADIUS servers failed to respond.

- Indicates likely network issue between SecureSync and Radius servers

wtmp.log

- File located in home/spectracom/log directory
- Records reboots and succesful logins/logouts,
- 0.0.0.0 indicates a local/internal connection. An IP address indicates external connection (ssh, browser, serial)
- File clears on each reboot/power cycl

What is the wtmp file (refer to: <http://linux.die.net/man/5/wtmp>)“

The *wtmp* file records all logins and logouts. Its format is exactly like *utmp* except that a null username indicates a logout on the associated terminal”

Example from our server

```
spadmin@Spectracom:/var/log
# 'pts/1 |D@V#uzpts/1ts/1spfactory10.2.100.234-V#
uzpts/-VbE[pts/1ts/1spadmin10.2.100.3F^V°
[pts/1UF^VGppts/1ts/1spadmin10.2.100.3cg^V!
ppts/1fh^V
,OptS/1ts/1spadmin10.2.100.3^i^V;c
,OptS/1Ei^V30F@pts/1ts/1spadmin10.2.100.124_Vc
dF@pts/;_VcPpts/1ts/1spadmin10.2.100.3?A_V#
ppts/10à_V#e8pts/1ts/1spfactory10.2.100.6°V)M
de8pts/1±8°V
8pts/1ts/1spadmin10.2.100.30R°VÙ
dANpts/2ts/2spadmin10.2.100.124è:»V#
d|spadmin@Spectracom /var/log $ PuTTYPuTTYPuTTYPuTTYPuTTY
PuTTYPuTTYPuTTY
```

Slightly modified Email (I added the word “successful” to “logins”) from Paul Myers (28 Feb 17)

This wtmp file records the reboots starts/stops, successful logins and logouts.

Every time a person logs in succesfully it is recorded.

If this file is large maybe they are automating a test login or they have provided a user account to an authenticated security scan to probe the unit or they are doing some type of automatic login and web scraping??

<http://www.linuxquestions.org/questions/linux-security-4/var-log-wtmp-72976/> <https://linux.die.net/man/5/wtmp>

(Note: Running the following tool converts the raw wtmp file to a readable binary file)

utmpdump /var/log/wtmp | less <enter> to review recent succesful logins. If the login is from a remote location, it will be associated with a specific IP address outside your network. Examples below:

additional notes

- Space to scroll
- Shift and q to quit

```
Spectracom log # utmpdump /var/log/wtmp
Utmp dump of /var/log/wtmp
[2] [00000] [^~] ] [reboot ] [^ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:05 2017 UTC]
[8] [00675] [rc ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:05 2017 UTC]
[1] [20019] [^~] ] [runlevel] [^~ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:05 2017 UTC]
[5] [02712] [l3 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:05 2017 UTC]
[8] [02712] [l3 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04267] [c3 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04268] [c4 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04269] [c5 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04270] [c6 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04271] [c8 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04266] [c2 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04265] [c1 ] ] [ ] ] [4.0.5-gentoo ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04265] [c1 ] ] [LOGIN ] [tty1 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04268] [c4 ] ] [LOGIN ] [tty4 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04269] [c5 ] ] [LOGIN ] [tty5 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04271] [c8 ] ] [LOGIN ] [tty80 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04270] [c6 ] ] [LOGIN ] [tty6 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04266] [c2 ] ] [LOGIN ] [tty2 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04267] [c3 ] ] [LOGIN ] [tty3 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 17:50:40 2017 UTC]
[7] [14654] [ts/2] ] [spfactory] [pts/2 ] ] [10.2.100.72 ] [ ] ] [10.2.100.72 ] [Tue Feb 28 21:29:15 2017 UTC]
[8] [14654] [ ] ] [ ] ] [pts/2 ] ] [ ] ] [0.0.0.0 ] [Tue Feb 28 21:31:30 2017 UTC]
Spectracom log #
```

Continued from Paul's Email above See the last 2 entries above?
 I logged into the unit using ssh and logged out.
 Logging into a serial port and staying logged in is shown below:

```

sufactories@spectracom ~$ sudo su
Spectracom@spectracom ~$ utmpdump /var/log/wtmp
Utmp dump of /var/log/wtmp
[2] [00000] [~~] [reboot] [~] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:05 2017 UTC]
[8] [00675] [rc] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:05 2017 UTC]
[1] [20019] [~~] [runlevel] [~] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:05 2017 UTC]
[5] [02712] [l3] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:05 2017 UTC]
[8] [02712] [l3] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04267] [c3] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04268] [c4] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04269] [c5] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04270] [c6] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04271] [s0] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04266] [c2] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04265] [c1] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04265] [c1] [ ] [LOGIN] [tty1] [ ] [ ] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04268] [c4] [ ] [LOGIN] [tty4] [ ] [ ] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04269] [c5] [ ] [LOGIN] [tty5] [ ] [ ] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04271] [s0] [ ] [LOGIN] [ttyS0] [ ] [ ] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04270] [c6] [ ] [LOGIN] [tty6] [ ] [ ] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04266] [c2] [ ] [LOGIN] [tty2] [ ] [ ] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04267] [c3] [ ] [LOGIN] [tty3] [ ] [ ] [0.0.0.0] [Tue Feb 28 17:50:40 2017 UTC]
[7] [14654] [ts/2] [sufactories] [lpts/2] [ ] [ ] [10.2.100.72] [ ] [10.2.100.72] [Tue Feb 28 21:29:15 2017 UTC]
[8] [14654] [ ] [ ] [ ] [ ] [ ] [ ] [0.0.0.0] [Tue Feb 28 21:31:30 2017 UTC]
[8] [04271] [s0] [ ] [ ] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 21:36:31 2017 UTC]
[5] [25123] [s0] [ ] [ ] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Tue Feb 28 21:36:31 2017 UTC]
[6] [25123] [s0] [ ] [LOGIN] [ttyS0] [ ] [ ] [0.0.0.0] [Tue Feb 28 21:36:31 2017 UTC]
Spectracom@spectracom ~$
  
```

To convert a wtmp file to a readable file

1. If it's a customer's wtmp file from a log bundle, FTP/SCP (using sufactories account and using "default" transfer mode) the wtmp file, into the **home/spectracom/log** directory of one of our units
2. Running the following tool converts the raw wtmp file to a readable binary file):

utmpdump /home/spectracom/log wtmp.log | less <enter> (where **wtmp.log** is the name of the wtmp log file desire to look at) to review recent logins. If the login is from a remote location, it will be associated with a **specific IP address** outside your network.

```



















utmpdump: cannot open /home/spectracom/log/wtmp1stn71: No such file or directory
sufactories@spectracom /var/log $ utmpdump /home/spectracom/log/wtmp1stn71.log | less
[2] [00000] [~~] [reboot] [~] [4.0.5-gentoo] [0.0.0.0] [Fri Aug 05 19:13:01 2017 UTC]
[8] [00663] [rc] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Fri Aug 05 19:13:01 2017 UTC]
[1] [20019] [~~] [runlevel] [~] [4.0.5-gentoo] [0.0.0.0] [Fri Aug 05 19:13:01 2017 UTC]
[5] [01223] [l3] [ ] [ ] [4.0.5-gentoo] [0.0.0.0] [Fri Aug 05 19:13:01 2017 UTC]
  
```

Notes

- Space to scroll
- Shift and q to quite

/Var/log directory (linux login logs such as lastlog)

- captured in both the Logs bundle and Configs bundles
- contains linux login log files (such as lastlog and faillog)

 apache2		11/8/2019 11:46 AM	File folder	
 sa		11/8/2019 11:46 AM	File folder	
 sandbox		11/8/2019 11:46 AM	File folder	
 .keep		3/14/2018 10:13 PM	KEEP File	0 KB
 dmesg		8/16/2019 1:45 PM	File	14 KB
 faillog		8/19/2019 12:15 PM	File	24 KB
 lastlog		6/18/2019 4:32 PM	File	0 KB
 rc.log		8/16/2019 1:46 PM	LOG File	60 KB
 wtmp		8/16/2019 1:46 PM	File	41 KB

Lastlog file is growing too large for configs bundle

- Refer to Salesforce Case 230530
- Fixed in 5.8.9 update (June 2020)

Email from Ron Dries (22 April 2020) Stuart was able to reproduce the issue Verizon is seeing here.

The lastlog file can become very large if a user with a very high UID logs into the SecureSync.

The lastlog file is a type of file called a sparse file, based on UID. What this means is that if a user has a high UID the lastlog file will generate space for all of the UIDs in between the large one and the next closest one.

What happens is that when the tar command gets to the lastlog file that has a very large UID, it generates a very large (hundreds of Gbs) file that takes up disk space causing the config bundle to not be able to be saved correctly.

The lastlog file does not need to be in the config bundle, so Engineering is working on a hotpatch that will ensure the lastlog file is not saved in the config bundle.

The patch should be available at the end of this week, and we can send it over to Verizon.

Chrony/chronyd

- Refer to “chrony/chronyd” in the Customerserviceassist doc: I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf
- Appears to replace NTP for linux systems. “chrony is a pair of programs for maintaining the accuracy of computer clocks. chronyd is a background daemon program that can be started at boot time.
- Link to “refclock_tsyncpci.c” file referenced in the email further below: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\chrony-chronyd (replacing NTP)
- The SecureSync doesn’t run Chrony. But it can sync Chrony clients.

Comparison of chrony, ntp and openntpd: refer to <https://chrony.tuxfamily.org/comparison.html>

Chronyd is a daemon which runs in background on the system. It obtains measurements (e.g. via the network) of the system’s offset relative to other systems, and adjusts the system time accordingly. For isolated systems, the user can periodically enter the correct time by hand (using *chronyc*). In either case, **chronyd** determines the rate at which the computer gains or loses time, and compensates for this.”

From <https://chrony.tuxfamily.org/>

Chrony is a versatile implementation of the Network Time Protocol (NTP). It can synchronize the system clock with NTP servers, reference clocks (e.g. GPS receiver), and manual input using wristwatch and keyboard. It can also operate as an NTPv4 (RFC 5905) server and peer to provide a time service to other computers in the network.

Compatibility of a Chrony client with a standard NTP time server (such as SecureSync)

Refer also to Salesforce case 24565

Email from Paul Myers (27 Feb 17) The SecureSync runs the NTP daemon standard implementation with the current release being 4.2.8p9 in Release 5.5.1

We do NOT run chrony on the SecureSync, however, a chrony client should be compatible. See the section 1.1 overview of manual which indicates it can support NTPv4 (RFC 5905)

<https://chrony.tuxfamily.org/comparison.html>

<https://chrony.tuxfamily.org/manual.html>

Time sources

	chrony	ntp	openntpd
NTP	Yes	Yes	Yes
Reference clocks	Yes	Yes	Yes
Manual input	Yes	No	No

Another example indicating how a Chrony client can sync to an NTP server is via Section 2: Installation of Chrony of the Chrony manual at” <https://chrony.tuxfamily.org/manual.html#Installation>

Now that the software is successfully installed, the next step is to set up a configuration file. The default location of the file is ‘/etc/chrony.conf’. Several examples of configuration with comments are included in the examples directory. Suppose you want to use public NTP servers from the pool.ntp.org project as your time reference. A minimal useful configuration file could be

```
pool pool.ntp.org iburst
makestep 1.0 3
rtcsync
```

NTP

- Good doc for definition of terms associated with NTP:
<http://support.ntp.org/bin/view/Support/NTPRelatedDefinitions>

NTP Versions in our software

Current version of NTP: <http://www.ntp.org/downloads.html>

- **NTP version in linux Gentoo package:** refer to <http://gentoobrowse.randomdan.homeip.net/package/net-misc/ntp>

NTP versions in SecureSync/9400s

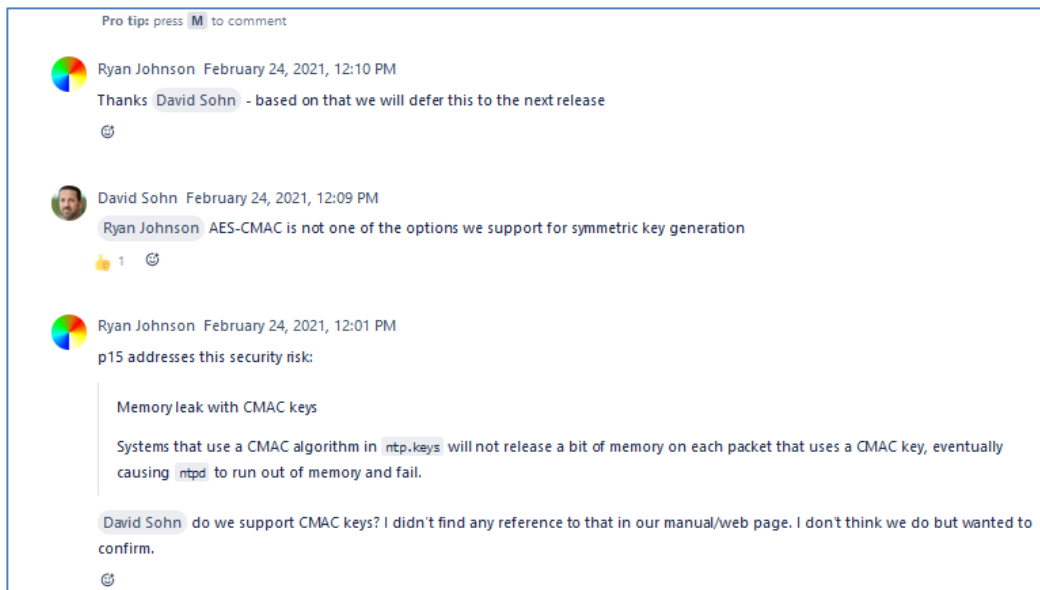
Refer also to: <I:\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates\Software release dates.xlsx>

Quick summary below (in descending order):

System Version	NTP version	Note
V5.9.3	Went to 4.2.8p15	Reference ECO-2958 (Nov 2021)
v5.9.1/5.9.2	No change to NTP. Still at 4.2.8p14	See note further below about 4.2.8p15 update not being incorporated yet.
v5.9.0	Went to v4.2.8p14	Reference ECO-2674 (Jan 2021)
v5.8.6	Went to v4.2.8p13	Reference ECO-FAI-2327 (Oct 2019)
v5.8.3	Went to v4.2.8p12	
v5.8.0	Went to v4.2.8p11	Reference ECO 1686. May, 2018
v5.7.0	Went to v4.2.8p10	Reference ECO 1270, ~8 Jun 2017
V5.6.0	No change to NTP	N/A
v5.5.0	Went to v4.2.8p9	Reference ECO 1112, ~Dec 2016
v5.4.5	Went to v4.2.8p8	Reference ECO 980, ~12 Sept 2016
v5.4.0	Went to v4.2.8p6	March, 2016
v5.3.0	Went to v4.2.8p3	
v5.2.1	Went to v4.2.8p2	
v5.0.0	Went to v4.2.6p5	
v4.8.9 and below	NTP v4.2.0	

Note about NTP version 4.2.8p15 not being incorporated in our version 5.9.1/5.9.2 updates

- Refer to **JIRA Ticket SSS-1006** (excerpted further below, in descending time order on 24 Feb 2021)
- In summary: We intentionally did not update to p15 in our version 5.9.1/5.9.2 update. At that time (~Feb 2021), p15 was fixing a function of NTP (AES-CMAC keys for Symmetric Key authentication, which had a memory leak issue) that SecureSync doesn't even support (we don't support AES-CMAC keys). So, Ryan Johnson made decision to hold off implementing p15, until a future software update.



NTP's timescale

- NTP output follows the System timescale (if the System Timescale is UTC, NTP output time will also be UTC)
- Unlike the 9300/9200 series (which can be independently configured to output UTC or GPS timescale) in at least versions 5.4.0 and below, NTP
- Changing the System Timescale to a different value (such as UTC to TAI) will cause ntpmond to force NTP to stop/restart because of the greater than one second error that will occur once the change is complete. A log entry should be asserted in the NTP log.

Statusd daemon for obtaining status info from NTP (v5.3.0 and above)

statusd (NTP status daemon)

Software update version 5.3.0 incorporated changes in how info from NTP is obtained for items such as the web browser, SNMP, the CLI interface and the front panel to report.

- Refer to mantis cases 3140 and especially 3067.
- The new statusd daemon was added in software version 5.3.0
 - Previously, several different threads were all calling NTPQ to get similar NTP status (NTP sync state, Stratum level, etc). Sometimes there could be too many calls to NTPQ. statusd limits the number of calls to only one thread which grab all of the status data and stores it in /tmp - giving all the other threads a centralized location to get the ntp data without having to use ntpq.
- statusd was initially called masterd but was renamed shortly thereafter to statusd (Mantis case 3094)
- Version 5.4.0 redesigned-improved statusd for lower CPU cycles.

Issue with too many threads calling NTPQ

Example System.log entries associated with an issue where NTPQ stops talking to NTP to get NTP status

Feb 23 15:37:12 ny4-apr-gps2 ny4-apr-gps2: [system] System command error: NTPQ_ReadSysstats (NTPAL)
Feb 23 15:37:12 ny4-apr-gps2 ny4-apr-gps2: [system] Failed to read NTP system statistics (NTPMOND)

Feb 23 15:39:34 ny4-apr-gps2 ny4-apr-gps2: [system] System command error: NTPQ_GetAsscVariable (NTPAL)
Feb 23 15:39:34 ny4-apr-gps2 ny4-apr-gps2: [system] NTPQ_GetAsscVariable(ASSC_VAR_LEAP) returned [rc = 1] (KHTD)

[system] System command error fpanel:DT_DrawStat (FPD) (only asserted if the front panel has been reconfigured to display NTP status info instead of network settings).

- Refer to Salesforce cases such as 19242, 19468 and 21098
- Symptoms of this issue with NTPQ include the above log entries,
 - “ntp status” CLI command no longer responding
 - Web Browser and SNMP not reporting NTP status
 - Front panel not able to display NTP status (if it’s been reconfigured to display NTP status).
- This issue was seen in software version 5.2.1 (reported in 5.3.0 as well, but likely due to a different reason)

This status information reported on the front panel (if the SecureSync has been configured to display Status information instead of the network settings, as many customers choose to display) includes the NTP Stratum and NTP Sync status.

Email Keith sent (12 Feb 16) Both the NTP Status CLI command stopping to respond and the “System command error fpanel:DT_DrawStat (FPD)” log entry are related to the SecureSync having earlier software version 5.2.1 installed, instead of the latest version of version 5.3.1 being installed.

Software versions 5.2.1 and below has several software threads running the NTPQ query tool to obtain similar status information from NTP (such as NTP sync status and Stratum level). Functions that all need to obtain this similar status info from NTP include the web browser, SNMP, CLI interface as well as the front panel LCD (when the front panel has been configured by a user to display NTP status info instead of the factory default setting of displaying network settings).

With all these functions calling NTPQ to get the NTP status, NTPQ could become overwhelmed with requests and therefore stop responding with this NTP status info (all other calls not needing NTP status info can continue to respond just fine while NTPQ is in this state). The “...fpanel:DT_DrawStat (FPD)” error message observed in the log is due to the front panel also trying to display NTP status info (just like the CLI command) but it’s not able to obtain the data from NTP.

Version 5.3.0 update added a new daemon called statusd, which centralized the request for NTP status info to a single thread, minimizing the number of instances of NTPQ needing to be run at the same time.

I recommend you consider updating the software to version 5.3.1 (or to version 5.4.0 when its released in a few weeks) to prevent this potential NTP status reporting condition from occurring. Note that in general, we recommend the SecureSync always have the latest version of software installed, as issues such as this are fixed with periodic updates we make available (we seldom remove functionalities with our software updates. The SecureSync updates add new capabilities and address potential software conditions that may be present. Customers with optional PSP packages or who have registered their contact info on our website are provided a notice when software updates become available☺!

Changes incorporated to statusd daemon

- **Version 5.3.0 update:** Created/added statusd to improve software CPU cycle usage.
- **V5.4.0 update:** Redesign of statusd and other daemons to improve software CPU cycle usage.
- **Version 5.4.5 update:** Modification of statusd to support NTPQ commands being issued in a single thread at a time.

Note: As indicated in SR 7112 and the associated logs, too many instances of NTPQ running in versions prior to
pg. 1130

v5.4.5 can apparently cause oops, bug, taint, call trace errors in kern log and eventually the out of memory manager killing apache to try to free up some additional memory.

Issues associated with statusd

- A) Versions prior to 5.4.5 may potentially run too many simultaneous instances of NTPD, resulting in oops.taint. call trace and eventual out of memory manager killing apache.
- B) Commanded shutdown resulted in system.log show statusd continuously restarting
- refer to Salesforce case 175134
 - below is example from system.log
- ```
Oct 1 19:50:35 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=23922, tid=b6fedb40): thread started (STATUSD)
Oct 1 19:50:35 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=23922, tid=b65ffb40): thread started (STATUSD)
Oct 1 19:51:42 ntp01sldcmo ntp01sldcmo: [system] statusd has started (STATUSD)
Oct 1 19:51:42 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=26580, tid=b6f57b40): thread started (STATUSD)
Oct 1 19:51:42 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=26580, tid=b65ffb40): thread started (STATUSD)
Oct 1 19:52:50 ntp01sldcmo ntp01sldcmo: [system] statusd has started (STATUSD)
Oct 1 19:52:50 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=29271, tid=b6f95b40): thread started (STATUSD)
Oct 1 19:52:50 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=29271, tid=b65ffb40): thread started (STATUSD)
Oct 1 19:53:58 ntp01sldcmo ntp01sldcmo: [system] statusd has started (STATUSD)
Oct 1 19:53:58 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=31988, tid=b6f09b40): thread started (STATUSD)
Oct 1 19:53:58 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=31988, tid=b65ffb40): thread started (STATUSD)
Oct 1 19:55:06 ntp01sldcmo ntp01sldcmo: [system] statusd has started (STATUSD)
Oct 1 19:55:06 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=2132, tid=b6f05b40): thread started (STATUSD)
Oct 1 19:55:06 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=2132, tid=b65ffb40): thread started (STATUSD)
Oct 1 19:56:14 ntp01sldcmo ntp01sldcmo: [system] statusd has started (STATUSD)
Oct 1 19:56:14 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=4744, tid=b6fa7b40): thread started (STATUSD)
Oct 1 19:56:14 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=4744, tid=b65ffb40): thread started (STATUSD)
```
- C) Setting the “Minimum CPU temperature” thresholds to above “100” causes statusd to continuously reset. Statusd continuously resetting prevents it from being able to provide NTP status info from NTPQ where necessary. NTP runs fine. But NTP status is reported as “??” because statusd keeps clearing out the values obtained from NTPQ.
- **"TemperatureThreshold"** settings (one for for Major alarm and one for Minor alarm) are in located in the **\config\temperature.conf** file

**Email Keith sent to a customer (4 Apr 16):** Please just make sure that the neither of the two **“Minimum CPU temperature”** thresholds (toward the bottom of the **Management -> Notifications** page of the browser, **System** tab) are sent to a value above **“100”**.

As of just this morning, we found the browser will allow you to set a value above the highest available setting of **“100”** (no error message is asserted when either or both is set to above **“100”**). But having either or both of these values set to above **“100”** will cause statusd (the status daemon for reporting status information such as from NTP) to keep restarting.

If either or both of these values is set to a value greater than 100, please set it back to the default value of **“100”**

and press submit to keep the status daemon from resetting.

---

## NTP Status Summary table (in the NTP Setup page)



- bottom-left side of the Management-> NTP Setup page of the browser

### “Selected Ref” field (NTP Selected Reference field)

**Software Issue (applicable to at least version 5.8.6 and below): “Selected Ref” field in this table not properly updating/refreshing to report NTP’s currently selected reference (can display a different reference)**

- Refer to Salesforce Cases such as **211506** (Oct 2019) as observed in v5.8.4 (and Dave L duplicated here in v5.8.6)
- NTP peers command (`ntpq -p`) is reporting the correct selected reference (“Selected Ref” field may be displaying a different reference altogether)
- Refer to JIRA SSS-724
- Rebooting the unit or restarting the unit causes the correct selected NTP reference to start being reported.

## Spectracom Reference Clock Driver (127.127.45.0)- “TSync(0)”

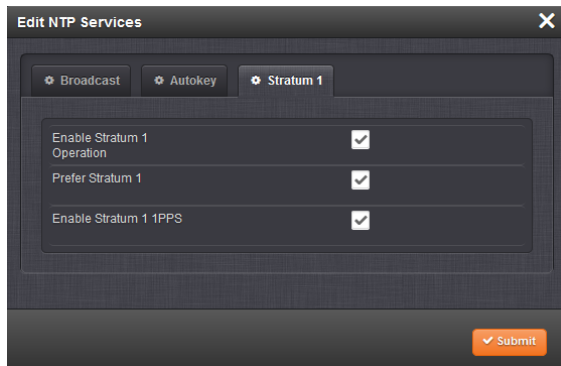
- Allows NTP to sync to System Time
- Enabled when the “timing System Reference ( *Management* -> *NTP Setup* page, “NTP Servers” tab) is Enabled.
- When enabled, adds a “System Time” row to the *Status* -> *NTP* page (as shown below).
- Reference ID (Ref ID) for the Spectracom driver reference is “.GPS”

127.127.45.0 is the Spectracom Reference Clock driver which allows NTP to obtain time from System Time.

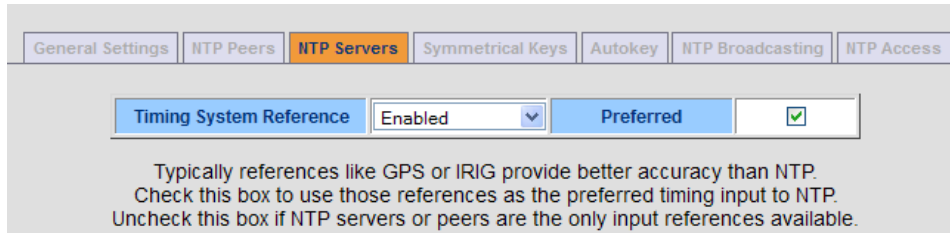
In SecureSync/9400 series

### C) Newer browser (v5.1.2 and above)

**Management** -> **NTP Setup** page of the browser (click the gear icon to the right of “NTP Services” and select the **Stratum 1** tab)



### Classic interface browser



In SecureSync/9400 series “NTP expert mode (versions 5.1.2 and above only)

server 127.127.45.0 prefer minpoll 4

(Note: “prefer” being present indicates the “preferred” checkbox is enabled)

In NTP log (when synced to System Time): `ntpd[826]: synchronized to PCI_TSYNC(0), stratum=0`

**Note:** The Reference Clock driver (127.127.45.0) is valid for NTP input when input references such as GPS, IRIG, Havequick, etc, are valid or if in Self mode. However, it's not valid when syncing SecureSync to other NTP servers.

## NTP Reference Status

| Sync | Host        | Ref ID | Stratum | LI | Mode   | Type  | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|-------------|--------|---------|----|--------|-------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| **   | System Time | .USER. | 0       | 00 | Client | local | none        | 3          | 16                  | 377   | 0.000      | 0.000       | 0.001       |

Version 4.7.0 change minpoll interval to “4 (16s)” for faster sync. The maxpoll is not specified, so according to Paul Myers, the poll interval is always every 16 seconds.

### Fudge stratum 1 (NTP normally goes to Stratum 1 when synced to GPS/Desire to change the Stratum value when synced with GPS/GNSS input)

- Not exactly sure why, but the NTP expert mode further below is not useable with v5.8.6 (works with 5.7.1 and 5.8.8):
  - **Per RonDries (27 Apr 2020)** We are not able to fudge the stratum level in v5.8.6, it looks like there is a problem with the Atom Clock Driver. You will see an error in the System Log “Apr 27 17:11:43 Spectracom ntpd[19388]: refclock\_newpeer: clock type 22 invalid”.
- Refer to Salesforce Case 22290 (April 2020) for Jasper with CME Group wanting the SecureSync to go to Stratum 3 (not 1), when synced with GPS:

#### Email from Dave L to Jasper (27 April 2020)

Yes, this will be the same change you made in the v5.7.1 config file.

Here is the config used at 5.8.8. it's the default config, just with the atom clock driver fudged to stratum 2: **just edit this one line “ fudge 127.127.22.0 stratum 2 “ (bolded further below)**

```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
tos orphanwait 1
tos orphan 15
server 127.127.45.0 prefer minpoll 3
server 127.127.22.0 minpoll 3
fudge 127.127.22.0 stratum 2
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logconfig=syncall +clockall +peerall +sysall
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats sysstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
filegen sysstats file sysstats type day enable
```

### Desire to fudge NTP to be Stratum 1 (instead of Stratum 2), while synced to another NTP server

Q We are doing the opposite. We are looking to make a Stratum 2 server to be a Stratum 1. The servers are NOT sync'ed to GNSS. They are sync'ed to Stratum 1 upstream servers.

**A reply from Keith (6 June 2020)** I completely understand. But I will need to check with our Apps Engineering team to see if NTP allows this capability.

From the quick testing I just performed, and from info I see online, NTP only allows a user to fudge a reference clock driver (inputs into NTP, other than from other NTP servers -such as the GNSS-synced time inside the SecureSync- are provided via several "types" of NTP reference clock drivers). These clock drivers tell NTP how to handle all the info its reference is providing it. NTP does not appear to support fudging the inputs values (such as the Stratum value) of other NTP servers.

NTP's stratum is always one higher than the stratum of its selected reference (whether that reference happens to be from a reference clock driver, such as the one for System time to sync NTP, or if its another NTP server).

For NTP to become Stratum 1, NTP within the SecureSync has to be synced to a reference indicating that it's a **Stratum 0 reference (or synced internally to itself with no outside reference)**. To NTP, stratum 0 normally tells NTP its an invalid NTP timestamp and to ignore it altogether as a reference. NTP allows Reference Clock drivers (but apparently not any other NTP servers) to fudge its Stratum to Stratum 0, so that NTP knows its still a valid reference. When NTP syncs to a fudged Reference Clock driver at Stratum 0, as usual, its NTP stratum goes to one higher than the reference (it goes to Stratum 1 because its reference is Stratum 0). However, in order to provide valid/useable NTP timestamps, other NTP servers can only report they are **Stratum 1** through **Stratum 15**. So, the highest Stratum that an NTP sever syncing to another NTP server can go is **Stratum 2**. In order for NTP to receive NTP timestamps from other NTP sever AND go to **stratum 1, the other NTP servers would have to announce they are Stratum 0 (an invalid reference)**.

This is a direct factor of NTP and not in any way a factor of the SecureSync. I will confirm with our Engineers that my understanding is completely correct, and to see if they are aware are any other possible work-arounds for NTP, which may allow NTP to report it's a Stratum 1 time server, even though its synced to other NTP sever (this is first request we've ever received to have this desired operation).

I will get back to you, once I hear back from them!

## NTP Orphan mode/orphanwait / Undisciplined Local Clock Reference (127.127.1.0)

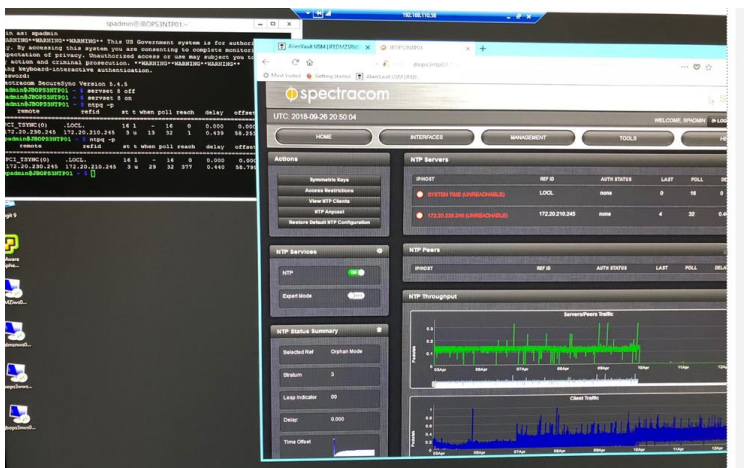
- Refer also to online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_Orphan.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_Orphan.htm)

### Orphan Mode (versions 5.2.1 and above)

- In software versions 5.2.0 and below, the NTP local clock reference was used to force NTP to go to Stratum 16.
- Orphan mode was added in NTP version v4.2.2 to replace the undisciplined Local Clock reference. So when we updated NTP to version 4.2.8p2 in software version 5.2.1, we had to start using NTP Orphan mode in its place.
- Orphan Mode allows a group of ntpd processes to autonomously select a leader in the event that all real time sources become unreachable (i.e. are inaccessible).
- Info about NTP Orphan mode, refer to: <http://www.eecis.udel.edu/~mills/ntp/html/orphan.html> and <http://support.ntp.org/bin/view/Support/OrphanMode>
- If there are no input references available for NTP to sync with, it will go into Orphan mode.

Indications of a time server being in Orphan mode are in the `ntpq -p` (peers command).

- The NTP refid will be **127.0.0.1**
- its NTP Reach value will **remain at "0"**.



Orphan Mode is enabled by adding the line "`tos orphan N`" anywhere in `ntp.conf`. The N specifies the stratum at which this `ntpd` will switch to Orphan Mode. For example, an `ntpd` using `tos orphan 6` will not switch to Orphan Mode as long as a time source of strata 1 through 5 is reachable. The recommended value for N is 2 less than the worst-case externally-reachable source of time.

In addition to the `tos orphan` line all members of the Orphan Mode group must be configured in a *mesh* (i.e. they must all be clients / peers of each other). Any NTP association mode may be used to set up this mesh.

**Email from Dave Sohn regarding a customer desiring SecureSync to be Stratum 4 when not in sync (30 Nov 15)**  
What SW version are they using? In more recent versions, there should be two additional lines in the `ntp` configuration file:

```
tos orphanwait 1
tos orphan 15
```

The second line "`tos orphan 15`" controls the out of sync stratum level. If they changed this to "`tos orphan 4`", the stratum level reported during the slewing, and when out of sync, will be 4. The functionality of NTP is such that even though it is slewing to the reference, it won't report the selection of the peer until it is closer in.

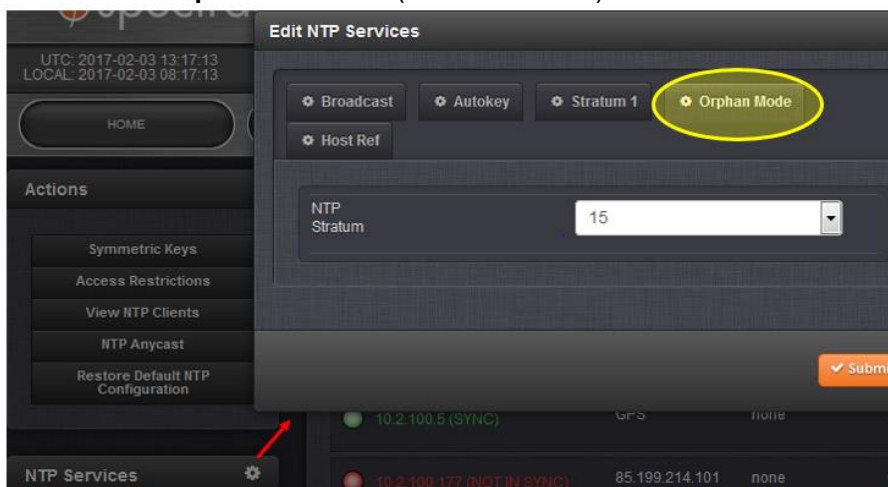


- **orphanwait 1** (our factory default setting is “1”) tells NTP to wait 1 second after losing all references before going into Orphan mode.

“Orphan Mode” configuration in the newer (black/charcoal) browser (can change what stratum NTP goes to when not in sync)

- Refer also to online SecureSync user guide at:  
[http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_Orphan.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_Orphan.htm)
- Factory default value is “15” (NTP clients won’t sync to this NTP server when NTP is not synced to a reference)

**Management** -> **NTP Setup** page of the newer browser. Press the gear ICON to the right of “NTP Services” and then select the “Orphan Mode” tab (as shown below):



Our Factory default settings for orphanmode and orphanwait settings

*(Regarding SF case 164267)*

**Per Dave Sohn (4 Jun 18) Orphanmode in 5.8.0 is still default of 15. The orphanwait setting is 1.**

---

## “Local Clock Reference (127.127.1.0)” enable/disable field

- Field is located in [Network](#) -> [NTP Setup](#) page of the browser, NTP Servers tab
- When enabled (default setting), NTP is allowed go to stratum 16 when input reference is either jittery or no input references are present.
- When disabled (not normally recommended) NTP will never go to Stratum 16. Its time stamps will never output as Stratum 0, so NTP clients won't ever ignore the time stamps as being questionable.
- When disabled, and if no other NTP inputs are present or not valid, NTP.log will insert an entry of “no servers reachable.”

Starting in Archive software version 4.8.6, a new enable/disable field has been added, in order to disable NTP's local clock reference (if needed or desired). Disabling this checkbox may help improve NTP operation when NTP's input reference(s) are not very stable or are periodically being lost.

The “Local Clock Reference” enable option determines whether or not NTP uses its Local Clock Reference as its selected reference, in the event all other references are lost or not selected due to stability, reliability or jitter. The Local Clock Reference degrades the NTP stratum to 15 by default when selected, so an NTP server without references cannot synchronize a timing chain of NTP servers.

When NTP selects the Local Clock Reference over any other external reference(s), NTP will go to Stratum 16 (by default). If NTP's inputs are not very stable (jittery) or are periodically not present, NTP may switch back and forth between Stratum 1 (or Stratum 2) and Stratum 16. While at Stratum 16, NTP will be ignored by the network clients. When it switches back to Stratum 1 or 2 again, it is considered a valid reference. An example where NTP may switch between an external reference and the Local Clock Reference is syncing SecureSync to an IRIG generator that is not externally synced to GPS, for instance. The IRIG input will not be jittery, resulting in NTP periodically selecting the Local Clock Reference over the IRIG generator, because the internal clock is more stable than the IRIG generator.

The Local Clock Reference can be disabled if the user does not desire this feature or to avoid switching between a reference and the Local Clock driver when the reference is intermittently reachable or less stable than the Local Clock. The Local Clock stratum can be adjusted to values other than 15 by using NTP Expert Mode.

### Effects on NTP when the System Time is manually changed to something else

I just ran a test to confirm what I expected to have happen, when the time is manually set while NTP is already running.

The time can't be manually set with any higher priority references being present and valid. So, for this test, I was initially synced to IRIG. I then disabled IRIG input and all references other than USER/USER. I then set the System Time ahead by about 6 minutes (this was at 10:04:07 Eastern).

At about 10:05:23 Eastern, NTP noticed System Time had jumped, because its offset value became a very high number. This caused NTP to momentarily go to Stratum 16, with no time jump occurring on the NTP outputs (still outputting the incrementing time, based on the time it was before the time was manually advanced). Time clients would still be syncing to it, still using the old time being incremented.

At about 10:08:53 Eastern, NTP went back to Stratum 1 with no time jump occurring on the NTP outputs (still outputting the incrementing time, based on the time it was before the time was manually advanced). Time clients would still be syncing to it, still using the old time being incremented.

This same operation continued (NTP still outputting the old time just incrementing) until about 10:22 Eastern, when NTP stepped its time to much closer to the manually set time. The NTP Offset significantly decreased at this point, but was not nearly 0. Jitter went up, as expected because of the large time change. This was about 17 minutes after I manually set the time.

Just after the step (about 10:23 Eastern), NTP temporarily went back to Stratum 16 again, but made a 6 minute time jump and the NTP packets advanced by about 6 minutes (still remaining at Stratum 16- NTP clients would ignore it right now).

At about 10:24:17 Eastern, NTP went back to Stratum 1 and the NTP packets were still 6 minutes ahead of the actual time, because the time had been manually set. NTP did adjust for the 6 minute time advance that I made happen by manually setting the time (though NTP doesn't like to do this). The Total elapsed time for when NTP Clients would see the time advance and be able to use the advanced time, was about 20 minutes after the manual set.

As I had mentioned, NTP takes quite a while to perform an unexpected time jump. In this case, it saw a 6 minute time difference than it expected to get from System Time. NTP said that its drift calculations must be WAY off, so it had to go through a process of recalculating the “error” in its calculations, in order for it to bring its time in alignment with the “new: System Time reference.

This is the expected operation for NTP when switching between references that are not closely aligned with each other.

**Note:** If the NTP input time changes while NTP is running, the poll interval will affect how long it takes for NTP to notice and adjust for an input time changes (the longer then poll Interval, the longer it will likely take).

---

### \*RFC 2783 (PPS clock driver, 127.127.22.0)

- Pulse-Per-Second API to discipline the Linux kernel.
- For more info, refer to <http://tools.ietf.org/html/rfc2783>
- PPS clock driver is 127.127.22.0

**Email from Dave Sohn (6 Feb 2013)** Starting in 5.0.2, we use an rfc 2783 interface for our timing system interface to source a 1PPS to NTP to discipline it.

**Q.** Is the SecureSync model we have compliant with RFC 2783 (attached)? If yes, is there any documentation we can show that proves it is?

**A (Reply From Keith)** Regarding your question about RFC 2783, the answer to this is: As of Archive software version 5.0.2, SecureSync does now use an RFC 2783 interface for our timing system to source a 1PPS signal to NTP, to discipline the Linux kernel.

---

### Signal 15 (“NTP Exiting on Signal 15”) or other signals

- Refer to <http://stackoverflow.com/questions/16723626/what-is-signal-15-received>
- This indicates the linux has delivered a SIGTERM to your process. This is usually at the request of some other process. This signal requests an orderly shutdown of your process (ntpd).

---

### Web browser NTP configurations

- D) Newer interface (5.1.2 and above): *Management* -> *NTP Setup* page
- E) Classic interface: *Management* -> *Network* -> *NTP Setup* page

---

### NTP drift file

- View NTP drift file in CLI: after going to /etc/ntp directory, type `cat ntp.drift <enter>`

## ntp.conf file

- Path to ntp.conf file: spectracom/etc/ntp
- View ntp.conf file in log bundle: spectracom/etc/ntp

## Default ntp.conf file settings and their purposes

### F) Example default ntp.conf file from version 5.2.1 (ntp v4.2.8p2)

- Includes configs for NTP Orphan mode, starting in version 5.2.1 (replaced NTP Local clock ref)

```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
tos orphanwait 1
tos orphan 15
server 127.127.45.0 prefer minpoll 3
peer 10.2.100.146 minpoll 3 maxpoll 3
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats sysstats
```

**tos orphanwait 1 and tos orphan 15:** configurations for NTP Orphan mode (replaced NTP local clock in version 5.2.1)

- **orphanwait 1** tells NTP to wait 1 second after losing all references before going into Orphan mode.
- **tos orphan 15** tells ntp to go to Stratum 15 when in Orphan mode

**restrict 127.0.0.1 and restrict :::1** You may need to add the following line to allow

**unrestricted access from the localhost** (so that you may monitor ntpd and perform on-the-fly configuration changes with ntpdc):

**noquery:** Ignore all NTP mode 6 and 7 packets (i.e., information queries and configuration requests) from the source.

**nomodify** Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

**Keys:** path to the NTP keys file.

**server:** References NTP can sync with (such as System Time, NTP's local ref or other time servers)

**fudge:** forces NTP to Stratum 1 when NTP is synced.

### G) Example default ntp.conf file from version 5.1.6 (ntp V4.2.6)

```

restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats

```

IPv4 configuration

IPv6 configuration

**restrict 127.0.0.1** and **restrict ::1** You may need to add the following line to allow unrestricted access from the localhost (so that you may monitor ntpd and perform on-the-fly configuration changes with ntpdc):

**noquery:** Ignore all NTP mode 6 and 7 packets (i.e., information queries and configuration requests) from the source.

**nomodify** Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

**Keys:** path to the NTP keys file.

**server:** References NTP can sync with (such as System Time, NTP's local ref or other time servers)

**fudge:** forces NTP to Stratum 1 when NTP is synced.

## Inhibit Ephemeral Peers (restrict nopeer)

- Requires NTP expert mode enabled (in at least v5.9.1 and below)
- Refer to Salesforce Case 256614
- Refer to: [https://kb.meinbergglobal.com/kb/time\\_sync/ntp/ntp\\_ephemeral\\_peer\\_associations](https://kb.meinbergglobal.com/kb/time_sync/ntp/ntp_ephemeral_peer_associations)  
<http://doc.ntp.org/current-stable/accopt.html#restrict>  
<http://doc.ntp.org/current-stable/accopt.html#restrict>

Note: The **nopeer** keyword was introduced in ntp-4.2.8p11, but only works as expected in **ntp-4.2.8p12** and later.

Per: <http://doc.ntp.org/current-stable/accopt.html#restrict>

nopeer

Deny packets that might mobilize an association unless authenticated. This includes broadcast, symmetric-active and manycast server packets when a configured association does not exist. It also includes `pool` associations, so if you want to use servers from a `pool` directive and also want to use `nopeer` by default, you'll want a "`restrict source ...`" line as well that does *not* include the `nopeer` directive. Note that this flag does not apply to packets that do not attempt to mobilize an association.

**Associated Email from Ron Dries (26 Jan 2021)**  
Hi Keith.

I investigated this and found the following information:

[https://kb.meinbergglobal.com/kb/time\\_sync/ntp/ntp\\_ephemeral\\_peer\\_associations](https://kb.meinbergglobal.com/kb/time_sync/ntp/ntp_ephemeral_peer_associations)

<http://doc.ntp.org/current-stable/acopt.html#restrict>

It looks like this occurs if a peer on the network that is not specified in the NTP config file directly/ but has the correct symmetric key the NTP server will add it automatically.

It looks like adding "restrict nopeer" to the NTP config file should stop this from happening. This can be done from NTP expert mode.

---

## Kiss of Death packets (KOD) for SecureSync/9400s

- Refer to the "KOD" section of Customerserviceassistance doc for general info on KOD
- Enabling "KOD in SecureSync requires editing the ntp.conf file in expert mode

Q (from Sylvain) I have received the following question about our NTP server capability (SecureSync) "**NTP server implementations should include the ability to return a KOD (Kiss-of-Death Packet) Packet**"

**Email from Dave Sohn (7 Oct 15)** Being able to send the KOD packet is an advanced configuration on SecureSync that can be enabled on a restrict line of the NTP configuration file while in expert mode.

**Reply from Sylvain to Dave S-** So I understand in your message that the function is possible.

The customer will have to use the Expert mode and enter some additional extended configuration command line.

Shall I understand that: the customer will have to know the text to enter? I mean: we don't provide the details of the text to enter – this is up to the customer to know what is the good text to enter depending on his system ?

I need this advice in order to anticipate the next question that the customer could ask to us...

**Reply from Dave Sohn** The kod flag is added on a restrict keyword line where kiss of death operation is desired. This is done in expert mode.

---

## NTP verification/NTP troubleshooting

### A) NTP Verification

#### **\*\*Clock Status / NTP precision value**

- Refer to "Clock Status / NTP precision value" in: [..\CustomerServiceAssistance.pdf](#)

### B) NTP Troubleshooting

#### 1. ntpq is reporting a peer/server's refID is remaining ".init"

- Refer to the NTP peering tech note: [.../EQUIPMENT/SPECTRACOM%20EQUIPMENT/SecureSync/NTP/NTP%20peering/](#)
- search this doc for "init" for more info
- in summary, one of the following conditions is likely occurring:
- the NTP Peer/Server is not reachable on port 123 or
- One SecureSync has the other configured as an NTP Peer -but its configured NTP peer isn't also configured to be peered back (NTP requires bi-directional peering, or the peer will be declared "init")
- Symmetric key authentication is being enforced but the peer/server are not authenticating successfully,

**Note:** an issue is being observed (~Jan 2019) in at least v5.8.2 that this condition is occurring if symmetric key authentication is enabled. not having authentication enabled allows peering to work fine.

---

#### 2. NTP reporting its "not in sync" / "Stratum 15", when it really should be reporting its "in sync"/"Stratum 1"

- Such as what occurred with Salesforce case 128576
  - **Description of this abnormal condition:** System is in sync with NTP enabled, but NTP is not reporting its not in sync, Stratum 15. NTP is likely able to sync NTP clients in this state, since its likely just an issue related to systemd/ntpq not being able to report the ntp status to the browser

**General troubleshooting recommendations for this abnormal condition:**

1. Try performing an **ntpq -p** (peers command) to see if it's able to report the status of ntp.
2. Try **restoring just the NTP configs** (via the button in the *Management* -> *NTP Setup* page of the browser) and see if NTP starts reporting its status correctly d within a few minutes of NTP being restarted (refer to SF Case 128576 in the specific examples directly below)
3. Optional: Try performing a clean command to restore all configs

**Specific examples of this abnormal condition occurring**

**C) System log full of ERROR reading StatusNTP.curLI empty string (KHTD)**

- Refer to SF case 128576

```
Mar 16 10:46:55 ADMN-SecureSync last message repeated 40 times
Mar 16 10:46:56 ADMN-SecureSync ADMN-SecureSync: [system] ERROR reading StatusNTP.curLI empty string (KHTD)
Mar 16 10:47:27 ADMN-SecureSync last message repeated 31 times
Mar 16 10:48:28 ADMN-SecureSync last message repeated 61 times
Mar 16 10:49:29 ADMN-SecureSync last message repeated 61 times
Mar 16 10:50:30 ADMN-SecureSync last message repeated 61 times
Mar 16 10:51:31 ADMN-SecureSync last message repeated 61 times
Mar 16 10:52:32 ADMN-SecureSync last message repeated 61 times
Mar 16 10:53:33 ADMN-SecureSync last message repeated 61 times
```

**Finding/fix for this issue:** Ron Dries saved a copy of the ntp.conf file and compared the saved conf file to the "default" ntp.conf file. He found a missing "restrict" line and some lines from an earlier version of NTP. Just performing a reset of the ntp configs fixed it the missing restrict line was preventing systemd from having permission to perform ntpq commands

---

**1. NTP peering issues (can't peer)**

- network routing/firewall issues
- peer not in sync
- NTP Symmetric key issues (wrong Key ID referenced/strings don't match/ selected hashing algorithms not the same on both device- such as MD5 on client and sha1 on the SecureSync)
- FPS 140-2 compliancy/issues with Symmetric key authentication/peering issues

**MAC decrypt: MAC length error**

- Refer to Salesforce Case 192055
- Customer experiencing issues peering 5.8.2 SecureSync with a Solaris box running NTP (two Solaris boxes peered OK)
- **System log also contained:** [system] ERROR! NTP generic status polling: Ntpq error: 6 NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ\_UTIL\_STATUS) (STATUSD)
- might be related to NTP FIPS Mode as described in this article??

[https://bugzilla.redhat.com/show\\_bug.cgi?id=1442083](https://bugzilla.redhat.com/show_bug.cgi?id=1442083)

**Using the ntpq -p or ntpq -pn commands (Peers commands)**

- Refer also to “NTPQ” in custassist doc for more info on this query tool: ..\CustomerServiceAssistance.pdf
- Open CLI and type **ntpq -p** <enter>

```

spadmin@Spectracom ~ $ ntpq -p
remote refid st t when poll reach delay offset jitter

10.2.100.177 .GPS. 1 u 1 8 3 0.286 0.016 0.004
spadmin@Spectracom ~ $

```

### NTPQ “accessibility”

By factory default settings (and for security purposes) ntpq commands are not accessible from any other machine outside the SecureSync (such as another SecureSync on the network or a networked Linux box, for examples). However, the SecureSync can perform ntpq peers commands for its own internal NTP, via its own CLI interface.

When performing the peers command on a SecureSync that you are connected to, don’t add its own address to the command (this will cause the command to fail, as your customer is reporting). Omitting its own address from the peers commands allow the commands to be successful (without the address being defined, ntpq in the SecureSync knows it’s a command intended for its own internal ntp- it doesn’t need the address to be included in the command),.

The example screenshot shows that when I enter the IP address of the SecureSync I’m logged into as part of the peers command, the command fails. But when I leave off the address from the peers command, the command is successful.

```

spadmin@Spectracom ~ $ ntpq -p 10.2.192.227
10.2.192.227: timed out, nothing received
***Request timed out
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ ntpq -p 10.2.192.227
10.2.192.227: timed out, nothing received
***Request timed out
spadmin@Spectracom ~ $ ntpq -p
remote refid st t when poll reach delay offset jitter

*PCI_TSINC(0) .GPS. 0 1 8 8 377 0.000 0.020 0.004
+10.2.192.226 .GPS. 1 u 6 8 377 0.231 0.004 0.290
spadmin@Spectracom ~ $

```

If there is a desire to allow ntpq commands to be accessible from “outside” the SecureSync itself (“ Allow NTP Queries”) refer to “NTP Access Restrictions” section of the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_AccsRestrict.htm?Highlight=allow%20queries](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_AccsRestrict.htm?Highlight=allow%20queries) (s croll down to “Allow NTP Queries” at the bottom of the page. By factory default, this checkbox is not selected. But a user can enable it, if they wish!!

### Reach value of “0”

#### Potential causes (see also refID of “.init”)

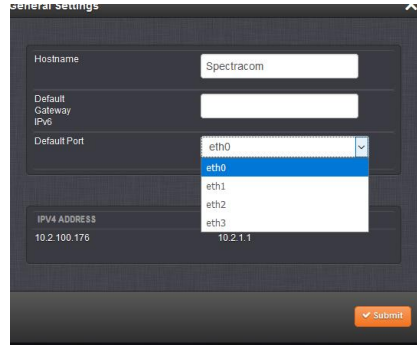
- NTP JUST started/restarted (first poll hasn’t occurr\_
- Port 123 closed on firewall in between the NTP servers
- Peers/servers configured with DNS names (instead of IP addresses) and there is an issue with DNS settings/operation (in the time sever or on the network – verify DNS is configured correctly in the SecureSync)
- Configured NTP Peer/Server is another Spectracom time server, and its NTP is not usable (Stratum 16)
- (if 1204-06 Gb eth card is installed) SecureSync’s main default port/default gateway is not configured correctly for thenetwork interface that has access to the configured NTP server/peer (such as to the Internet for an internet time server)
- Symmetric key authentication being enforced but keys not correctly configured



- One server is peered with another server- but the other server isn't also configured to have the first one as its peer, as well (A is peered with B, but B is not peered with a). Peering is bi-directional.
- 

### Steps/Suggestions to troubleshoot "Reach 0"

1. (if 1204-06 Gb eth card is installed) verify SecureSync's main default port/default gateway is not configured correctly (**Management -> Network Setup** page, **General Setting** button)



2. In the CLI, perform a **traceroute** command (refer to info/example further below)

- Refer to [tracepath and traceroute commands](#) (in this doc) for more info on this command.
- Refer to: <https://linux.die.net/man/8/tracepath> for available switches

Type: **traceroute -p 123 xxxx** (where -p 123 defines NTP port and xxxx is the IP/hostname of the peer/server), should respond with list of responses all the way to the peer/server

**traceroute -p 123 time.spectracomcorp.com** As shown below, verify the last value is **74.112.39.70** followed by "reached" at the end of the line:

```
Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
1?: [LOCALHOST] pmtu 1500
1: 10.2.1.1 2.353ms
1: 10.2.1.1 2.239ms
2: 74.112.39.70 2.165ms reached
Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

### Example of a destination address not being available via port 123 ("send failed" to a bad address)

```
spadmin@Spectracom ~ $ tracepath -p 123 10.1.2.8
1: send failed
Resume: pmtu 65535
spadmin@Spectracom ~ $
```

What is the "Reach" value for "nytime" (its row) in this ntpq -q response? Note it should be "377" if it can get receive good NTP packets from nytime (such as what is being reported in the second row of the screenshot above). If it's a "0", this SecureSync is not getting any NTP packets from nytime, or the NTP packets are indicating nytime is not in sync/Stratum1

The response to this command should list nytime's IP address/DNS host name in the first column. First try pinging this value (exactly as shown in the ntpq -p response) from the command prompt to ensure there is a response from nytime to this SecureSync.

Then at its command prompt, type the following: **tracepath -p 123 time.spectracomcorp.com** As shown below, verify the last value is **63.138.60.57** (note this IP address may vary) followed by "reached" at the end of the line:

```

Resume: pmtu 1500 hops 1 back 64
spadmin@spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
1?: [LOCALHOST] pmtu 1500
1: 10.2.1.1 2.353ms
1: 10.2.1.1 2.239ms
2: 74.112.39.70 2.165ms reached
Resume: pmtu 1500 hops 2 back 63
spadmin@spectracom ~ $

```

Repeat this same command above, but replace “time.spectracomcorp.com” (at the end of the command) with the exact IP/hostname for “nytime” (As reported in the ntpq -p response). The last value in this response should be the IP address of “nytime” (instead of 74.112.39.70) followed by “reached” at the end of the line (assuming nytime

3. Use **tcpdump** (via CLI) to confirm NTP requests are going out and if they are being returned (and if they are going out the correct port).

The following command (v5.4.5 and above. If v5.4.1 or below, add “:sudo” to the beginning) should show all NTP packets being sent and/or received on any of the network interfaces (eth0 and/or eth1/eth2/eth23 if 1204-06 card is installed): **tcpdump -i any port 123** (ctrl + c to stop the capture)

**Note:** if tcpdump responds with a password, tcpdump has disabled (and can't be re-enabled without performing a full update/restore to defaults)

## Using the “**ntpdate**” command

- cannot be performed by spadmin, but “**ntpdate -d**” can be performed by spadmin
- Refer to sites such as [http://www-01.ibm.com/support/knowledgecenter/ssw\\_aix\\_61/com.ibm.aix.cmds4/ntpdate.htm](http://www-01.ibm.com/support/knowledgecenter/ssw_aix_61/com.ibm.aix.cmds4/ntpdate.htm)
- On a linux box, use the ntpdate command in debug mode (ntpdate -d xxx.xxx.xxx.xxx) to verify info in NTP packet.
- Reports info such as Stratum, delay, offset, refid, etc.

### ntpdate

**Internal use only:** When using one of our SecureSyncs to perform this command, have to be logged in as root (not spadmin or spfactory) to perform “**ntpdate**”. But don't need to be logged in as root to perform “**ntpdate -d**”.

```

root@Custservice177:/home/spectracom
spfactory@Custservice177 ~ $ sudo su
Custservice177 spectracom # ntpdate 10.2.100.156
 8 Apr 21:56:26 ntpdate[20461]: the NTP socket is in use, exiting
Custservice177 spectracom # ntpdate -d 10.2.100.156
 8 Apr 21:56:31 ntpdate[20879]: ntpdate 4.2.6p5@1.2349-o Fri Jan 30 15:51:28 UTC
2015 (1)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
server 10.2.100.156, port 123
stratum 1, precision -19, leap 00, trust 000
refid [PPS], delay 0.02655, dispersion 0.00012
transmitted 4, in filter 4
reference time: d8d0228d.06a930ec Wed, Apr 8 2015 21:56:29.026
originate timestamp: d8d0229c.7a065162 Wed, Apr 8 2015 21:56:44.476
transmit timestamp: d8d02295.ebd015ac Wed, Apr 8 2015 21:56:37.921
filter delay: 0.02678 0.02655 0.02657 0.02658
 0.00000 0.00000 0.00000 0.00000
filter offset: 6.554613 6.554595 6.554718 6.554832
 0.000000 0.000000 0.000000 0.000000
delay 0.02655, dispersion 0.00012
offset 6.554595

 8 Apr 21:56:37 ntpdate[20879]: step time server 10.2.100.156 offset 6.554595 se
c
Custservice177 spectracom #

```

---

## Verifying if NTP is actually running

To see if NTP is running, type **ps -el | grep ntp <enter>** (where it will list everything with the name typed after "grep):

```
admin@Spectracom /etc/init.d $ ps -el | grep ntp
S 0 3455 1 0 77 -3 - 1205 poll_s ? 00:03:43 ntpd
S 0 3893 1 0 80 0 - 1102 poll_s ? 00:00:24 ntpmond
S 0 17337 17332 0 80 0 - 680 poll_s ? 00:00:00 ntp
admin@Spectracom /etc/init.d $
```

**Note:** Not all of the "NTP" services will be running all the time. NTPQ will only periodically be listed.

```
admin@Spectracom /etc/init.d $ ps -el | grep ntp
S 0 3455 1 0 77 -3 - 1205 poll_s ? 00:03:42 ntpd
S 0 3893 1 0 80 0 - 1101 hrttime ? 00:00:24 ntpmond
S 0 10067 10065 1 80 0 - 680 poll_s ? 00:00:00 ntp
admin@Spectracom /etc/init.d $
```

**Note:** when the NTP enable/disable switch is off, NTP should be stopped (not listed)

---

## **\*\*Logs for NTP**

- Refer also to: [NTP.log entries \(NTP Log entries\)](#)

### **3. ntp.log (displayed in browser and part of log bundle)**

Refer to **ntp.log** in the “Logs” section of this document ( [NTP log](#)) for examples and additional info

### **4. Daemon.log (not displayed in browser but part of the log bundle)**

- Get a full log bundle
- Logs state changes for the NTP daemon
- Refer to daemon.log in the “Logs” section of this document for examples and additional info

---

## **NTP Setup page doesn't show any fields (like a black page)**

- NTP Expert mode is likely enabled (If not using Expert mode, disable it to see the fields again)

---

## **\*\*Home page intermittently not showing NTP Stratum**

- Left side of the Home page of the browser should always display NTP stratum value (if NTP is running)
- In at least versions 5.1.5 and below:
  - If there are any alarms asserted, the Stratum value will be reported on this page.
  - If there are NO alarms asserted, the Stratum value will not be reported on this page.

---

## **\*Dedicated NTP input- periodic Holdover alarms being asserted**

- Refer to Salesforce case 18014 for Kaiser Permanente
- Dedicated Stratum 2 SecureSync was periodically going into Holdover for a very short period of time (like a second or two). Then was fine again.
- Cause: “It appears that the network switch port for this unit was incorrectly configured and the eth0 interface was only operating at 10/half. It is now auto-negotiated to 100/Full and the problem seems to have gone away.”

---

## **\*\*NTP Peering (NTP Peers and NTP Servers)**

### **Apparent/potential Issue with peering SecureSyncs when Symmetric key authentication is enabled**

- observed “in the field” and here around Jan 2019, with 5.8.2 installed
- Refer to Salesforce cases such as 178428
- Refer to JIRA SSS-586

**Status Update: Ron D tested this here with two SecureSyncs with Symmetric key enabled- worked just fine ???**

---

### **\*\*\*\*the newer browser doesn't provide the ability to edit/delete any NTP Peers or Servers**

**Solution:** May need to first disable NTP (**Management** -> **NTP setup** page of the browser). After deleting/editing the NTP peers or servers, re-enable NTP again.

**Email from Dave L (19 Jan 17)** I worked with Rick this morning and was able to delete the Servers and Peers from the unit. All I had to do was turn off NTP using the switch on the NTP Setup page and turn it back on again. The NTPQ -p did not show them anymore.

---

### **\*\*\*\*NTP peering of SecureSyncs in Simulcast applications**

- Due to what NTP peering will do the 1PPS and other associated outputs, NTP Peering of SecureSync Master Oscillators in Simulcast applications is NOT recommended! The only viable input reference should be GPS.

If GPS is lost and the unit is peered with any other server, no matter what type oscillator is installed (Rubidium, OCXO or TCXO) the System PPS (and therefore all outputs based on the System PPS ontime point) is dithered (not slowly slewed) from where it is to where NTP's 1PPS is. This jumping of the System PPS to align with NTP and will adversely affect simulcast radios that are synced by the SecureSyncs 1PPS and other outputs.

---

### **NTP peering/stratum synchroniation with a “unidirectional data diode in between the NTP devices**

- Refer to Salesforce Case 231161 (April 2020)

Q “We have 2 SecureSync appliances (1200-011) , both having the Gigabit Ethernet (3 port) option module (1204-06). They are separated by a unidirectional data diode. Is there anyway to sync ntp appliance B from ntp appliance A if a 1-way data diode is between them?”

**A Reply from Ron Dries (28 April 2020)** Broadcast mode may work in this situation but I am concerned that the clients will still try to send requests back to the server to compensate for network delay.

With them already having SecureSyncs it could not hurt to try and configure broadcast on the devices to see if it will work.

They will need to configure both the client and server for broadcast, and because packets won't be able to go back and forth the accuracy is not going to be good if it works.

The configuration will require expert mode on the client side to add the “broadcastclient” option, and we also recommend they use symmetric keys on both for security.

**Keith's response to customer:** Thanks for your great question pertaining to the desire to sync one SecureSync to another SecureSync via NTP, separated by a unidirectional data diode (our Case Number\_231161).

This “data diode” was a first for me. I had a thought on a potential method for this to work, but wasn't certain on it. So I forwarded your question over to our Apps Engineering team for their input. Before I could respond to let you know I was looking into it, one of the Engineers has already gotten back to me 😊!!

FYI: NTP sync is normally bi-directional, with an NTP request sent, followed by an NTP response. This helps NTP compensate for the path delays in between the two devices (though NTP needs to assume the delays are the same in both

directions). NTP can optionally operate in a broadcast only mode where NTP packets are sent unsolicited from one NTP server via the network's broadcast address. All NTP slaves listening to the broadcast address can then receive NTP timestamps. This operation prevents NTP from being able to calculate/account for path delays in between the NTP client and NTP server, so its inherently less accurate than bi-directional NTP operation.

NTP Broadcast mode may work in this situation, but the Engineer is concerned that the NTP client(s) will still try to send requests back to the NTP server SecureSync to compensate for network delay.

With you already having SecureSyncs installed, it certainly cant hurt to try and configure NTP broadcast mode on the SecureSyncs to see if it will work for you!

You will need to configure both the NTP client SecureSync and NTP server SecureSync for NTP broadcast mode, and because packets won't be able to go back and forth, he also mentioned the inherent accuracy degradations I mentioned above.

The configuration will require NTP Expert mode on the NTP client SecureSync to add the "broadcastclient" option, and we also recommend you use symmetric keys (shared ASCII key strings) on both SecureSyncs for enhanced security.

Attached you should find two documents. The first document is regarding NTP client/server sync and NTP peering, which is for two or more NTP servers which can sync back and forth to each other).

Section 1 of the other document discusses how to enable NTP expert mode (note that this mode needs to remain enabled, or changes made while in Expert mode will be lost) while Section 2 discusses how to enable NTP broadcast mode.

Please let me know if the NTP broadcast mode works for your particular application!! Thanks in advance!

To add to my last reply, I forgot to add a third document to reference. This third document discusses how to optionally configure symmetric key (NTP authentication) recommended for enhanced security.

Essentially, symmetric key authentication tells NTP whether its NTP server can be "trusted" as its time source, because The NTP server knows the same ASCII key string that's also configured in the NTP client.

Having incorrect or no hashes included in the NTP packets is an indication the NTP server may be an "imposter" time sever which cant be trusted.

---

### **Desire to configure/add peers and servers but not allow NTP to ever select them as its time source (such as just to monitor the stats of some other severs)**

Q Lastly, is there any way for us to define 10 ntp servers, but restrict the spectracom device to only use 3 out of 10 servers to steer its clock? We want to see statistics for the other 7 servers but we don't want it to steer the clock. Is it possible?

Can this be accomplished using expert mode and passing in the "noselect" option in the ntp.conf file?

A **Reply from Keith (6 March 2019)** Based on online documentation about the ntp.conf file (<https://linux.die.net/man/5/ntp.conf>) this looks like a great solution to be able to monitor NTP servers without them being selected by NTP.

## \*\*\*\*NTP Peers and NTP Servers status/Limited Reach/unreachable server

### D) Newer black/charcoal web browser (versions 5.1.2 and above)

*Management* -> *NTP Setup* page of the browser

The screenshot shows two panels from the NTP Setup page. The top panel, titled 'NTP Servers', contains a table with two entries, both in sync. The bottom panel, titled 'NTP Peers', contains a table with two entries; one is in sync and the other is not.

| IP/HOST            | REF ID | AUTH STATUS | LAST | POLL | DELAY (MS) |
|--------------------|--------|-------------|------|------|------------|
| SYSTEM TIME (SYNC) | .GPS.  | none        | 7    | 16   | 0.000      |
| SYSTEM 1PPS (SYNC) | .PPS.  | none        | 5    | 16   | 0.000      |

| IP/HOST                     | REF ID | AUTH STATUS | LAST | POLL | DELAY  |
|-----------------------------|--------|-------------|------|------|--------|
| 10.2.100.176 (SYNC)         | .PPS.  | none        | 2    | 16   | 0.205  |
| 198.60.22.240 (NOT IN SYNC) | .GPS.  | none        | 2    | 8    | 68.460 |

This screenshot shows the 'NTP Peers' table with two entries. Both entries are marked as 'LIMITED REACH' with a yellow circle icon.

| IP/HOST                       | REF ID | AUTH STATUS | LAST | POLL | DELAY  |
|-------------------------------|--------|-------------|------|------|--------|
| 10.2.100.176 (LIMITED REACH)  | .PPS.  | none        | 10   | 16   | 0.226  |
| 198.60.22.240 (LIMITED REACH) | .GPS.  | none        | 1    | 8    | 68.485 |

Number of listed peers/servers displayed in the Servers/Peers tables doesn't match the response to ntpq -p commands

- **ntpq -p** and **ntpq -pn** CLI commands report a list of **all configured** NTP Servers and NTP Peers
- **NTP Setup page:** to help simplify the NTP Setup page of the browser, it only lists/displays the configured servers/peers having a reach value **greater than "0"**. **Unreachable** peers/servers (reach of "0", or reach is "377" but the other time server isn't in sync) are not displayed in the browser. even though ntpq command does list them

Servers/peers being reported as an **Unreachable**

- Occurs when:
  1. Peers/Servers have a Reach of "0" (no time stamps being received back from this other time server) OR
  2. Reach is **not "0"** (such as "377" for instance), but this other NTP time server isn't in sync (its NTP may be in "Orphan mode" because it has no references it can sync with. So, its still providing timestamps, but its Stratum value is being reported as Stratum 0 (invalid/not useable)

---

## Color coding/labeling of each listed peer and server

### Notes:

- 1) Per Ron Dries: Color coding of each reference is based on the NTP Tally code and Reach value for each.
- 2) The tally code is determined by NTP's "Clock Select" Algorithm (refer to <https://www.eecis.udel.edu/~mills/ntp/html/select.html>). This algorithm performs sanity checks on each reference to decide which are "sane" candidates and which are "insane".

### By factory default, only a total of four NTP Peers/Servers will be listed in green

- The Clock Select algorithm (by NTP default settings) will select up to (3) three sane servers and (1) one candidate. All others are then marked as "non-candidates". So up to four total Peers/Servers will be in green by default. The rest will be red.
- See additional info further below on how to make more than four peers be in green.

---

### While trying to peer two SecureSyncs NTP disqualifying TSync (GPS) reference as well as the NTP peer due to large time difference between the two (NTP put an "x" in front of both references so neither could be selected).

- Customer had two SecureSyncs in two different countries. There was about an 800ms offset between NTP and the TSync driver. NTP wouldn't choose either one (it was rejecting both references because the error was so large and it only had two references). If the Peer was turned off, both synced to GPS just fine.
- Paul recommended changing the NTP peer's minpoll to 6 and its maxpoll to 10, to provide NTP with a little extra time to select TSync while it was still qualifying the peer (its Reach was still low when it selected NTP in our test case (we peered with a unit in Texas to generate a 200ms difference between TSync and NTP

---

## TOS command

### Minsane and Minclock: Ability to increase the number of peers that can turn green (all others being "falsetickers")

- Refer to <https://www.eecis.udel.edu/~mills/ntp/html/select.html> and <https://docs.ntpsec.org/latest/miscopt.html>
- Refer to cases such as 283635.
- Can alter the number of lines that can be green (candidates) instead of red (falsetickers) via NTP Expert mode (to be more than four total, the default number)
- Add the following line to the ntp.conf file (as shown below) after enabling NTP Expert mode: **tos minclock 6 minsane 6** (where 6 and 6 will allow up to 12 total references that can turn green).

Excerpt below is from <https://docs.ntpsec.org/latest/miscopt.html>

```
tos [ceiling ceiling | floor floor | maxclock maxclock | maxdist maxdist | minclock minclock | mindist mindist |
minsane minsane | orphan stratum | orphanwait delay]
```

This command alters certain system variables used by the clock selection and clustering algorithms. The default values of these variables have been carefully optimized for a wide range of network speeds and reliability expectations. Very rarely is it necessary to change the default values; but, some folks can't resist twisting the knobs. It can be used to select the quality and quantity of peers used to synchronize the system clock and is most useful in dynamic server discovery schemes. The options are as follows:



ceiling *ceiling*

Specify the maximum stratum (exclusive) for acceptable server packets. The default is 16. See the [Automatic Server Discovery](#) page for further details.

floor *floor*

Specify the minimum stratum (inclusive) for acceptable server packets. The default is 1. See the [Automatic Server Discovery](#) page for further details.

maxclock *maxclock*

Specify the maximum number of servers retained by the server discovery schemes. The default is 10, which should typically be changed. This should be an odd number (to most effectively outvote [falsetickers](#)) typically two or three more than `minclock`, plus the number of `pool` entries. The pool entries must be added as `maxclock`, but not `minclock`, also counts the `pool` entries themselves. For example, `tos maxclock 11` with four `pool` lines would keep 7 associations. See the [Automatic Server Discovery](#) page for further details.

maxdist *maxdistance*

Specify the synchronization distance threshold used by the clock selection algorithm. The default is 1.5 s. This determines both the minimum number of packets to set the system clock and the maximum roundtrip delay. It can be decreased to improve reliability or increased to synchronize clocks on the Moon or planets.

maxdisp *maxdispersion*

Specify the maximum dispersion used by the clock synchronization algorithm. The default is 16 s. This is also the dispersion assigned to missing data. See RFC 5905 for discussion.

minclock *minclock*

Specify the number of servers used by the clustering algorithm as the minimum to include on the candidate list. The default is 3. This is also the number of servers to be averaged by the combining algorithm.

mindist *mindistance*

Specify the minimum distance used by the selection and anticlockhop algorithm. Larger values increase the tolerance for outliers; smaller values increase the selectivity. The default is .001 s. In some cases, such as reference clocks with high jitter and a PPS signal, it is useful to increase the value to insure the intersection interval is always nonempty.

minsane *minsane*

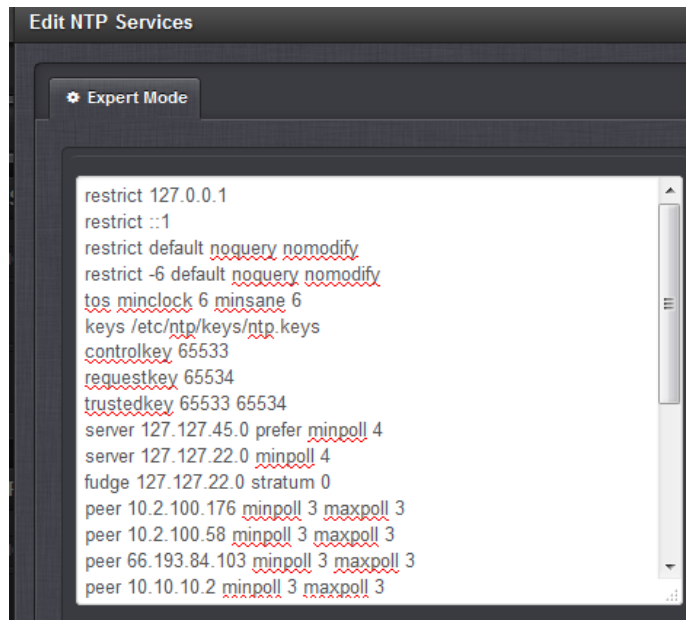
Specify the number of servers used by the selection algorithm as the minimum to set the system clock. The default is 1 for legacy purposes; however, for critical applications the value should be somewhat higher (e.g. 3) but less than `minclock`.

orphan *stratum*

Specify the orphan stratum with default 16. If less than 16 this is the stratum assumed by the root servers. See the [Orphan Mode](#) page for further details.

`orphanwait` *delay*

Specify the delay in seconds from the time all sources are lost until orphan parent mode is enabled with default 300 s (five minutes). During this period, the local clock driver and the modem driver are not selectable, unless marked with the `prefer` keyword. This allows time for one or more primary sources to become reachable and selectable before using backup sources, and avoids transient use of the backup sources at startup.



```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
tos minclock 6 minsane 6
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
peer 10.2.100.176 minpoll 3 maxpoll 3
peer 10.2.100.58 minpoll 3 maxpoll 3
peer 66.193.84.103 minpoll 3 maxpoll 3
peer 10.10.10.2 minpoll 3 maxpoll 3
```

As for “falseticker” (and the desire to point each SecureSync to multiple other time servers) I have some additional information for you...

In summary of the info below, what you are observing is the normal operation of NTP (without an optional user modification to the `ntp.conf` file via NTP Expert mode. NTP "Expert mode" is what allows a SecureSync user to make changes to the `ntp.conf` file beyond the available fields in the Management -> NTP Setup page of the browser).

For more info on NTP "**Minsane**", please refer to the NTP documentation at: <https://www.eecis.udel.edu/~mills/ntp/html/select.html>.

For more info on enabling NTP expert mode, please refer to the online SecureSync user guide at: [https://orolia.com/manuals/SS/Content/\\_Global/Topics/NTP/NTP\\_ExpertMode.htm](https://orolia.com/manuals/SS/Content/_Global/Topics/NTP/NTP_ExpertMode.htm)

*Please note that once NTP Expert mode has been enabled and any changes made to the `ntp.conf` file, NTP Expert mode must remain enabled from that point forward. If its disabled thereafter, any edits that were made to this file while in Expert mode will be lost. While NTP Expert mode is enabled, many of the fields in the Management -> NTP Setup page of the browser will no longer be controllable from this web page, as they are now controlled directly by the `ntp.file`.*

In general and as an FYI- we do not recommend configuring a SecureSync that is normally synced with GPS (Stratum 1) to more than 4 or 5 at most, other NTP servers for NTP peering. Though GPS is a “preferred” reference for NTP, having too many NTP servers listed as peers can cause them to “out-weigh” the GPS input into NTP. So instead of NTP syncing with the GPS time (System Time) it may instead select an NTP peer over GPS as its reference just because of the number of NTP servers it also has

available. If it selects an NTP server over GPS, the SecureSync will switch from Stratum 1 to Stratum 2 and its NTP accuracy capability will also inherently decrease because NTP input is not nearly as accurate as GPS input. Limiting the number of configured peers to approximately 3 or 4 will help prevent NTP from syncing to another NTP server over the GPS synced System Time while GPS reception is present.

For a dedicated Stratum 2 server (no GPS input) there's no reason not to list several NTP servers as peers, so that NTP always has several to choose from. But with a Stratum 1 server, its recommended (though not required) to limit the number of listed peers to three or four other NTP servers for redundancy.

As for falseticker, this is associated with the NTP algorithms used to select which reference it syncs with and which other references are still available as candidates for selection in case NTP decides that a candidate becomes a better reference than its currently selected reference. NTP can choose to switch to another reference, as it feels best, based on many parameters (Stratum level, jitter and offset, etc).

NTP is always qualifying all of its listed/available reference for selection of one reference to sync with. It does this by selecting four of the best ones and declaring the others as "falsetickers" (or "outliers"). It selects one of the four remaining as its reference and the other three remaining are considered candidates. An outlier isn't selected at that time for its sync. But as NTP continues to qualify all of its references, it may change a falseticker to a candidate or may select it as its reference, at any time. So even though a peer is currently a falseticker doesn't mean it is bad or can't be selected at a different time.

This means that up to four total references can be displayed as green in the web browser. But a red reference can turn green and a green one can turn red, as NTP sees best.

This is based on the default configuration of NTP. It can be changed, if desired with the use of NTP Expert mode (note that in Expert mode, most of the GUI settings for NTP will no longer be available and if Expert Mode is ever disabled, the NTP configuration will be restored back to the factory configuration). Adding a line to the ntp.conf file will allow all peers NTP feels are candidates for selection to be green, instead of just up to four. Though the default configuration still allows any peer to be selected at one time, this change allows more peers to be considered candidates at any one given time (more of them can be green).

As shown below, enabling expert mode and then adding the following line to the ntp.conf file will allow up to 12 total peers to be green at any given time, as long as NTP considers them good: **tos minclock 6 minsane 6**. Note the SecureSync user manual discusses how to enable NTP Expert mode.

```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
tos minclock 6 minsane 6
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
peer 10.2.100.176 minpoll 3 maxpoll 3
peer 10.2.100.58 minpoll 3 maxpoll 3
peer 66.193.84.103 minpoll 3 maxpoll 3
peer 10.10.10.2 minpoll 3 maxpoll 3
```

---

NTP Tally code

| Tally code | Green = (Sync)<br>Red = (Not in Sync) (if the Reach is not 0)                                                                         | Truechimer (good) or<br>falseticker (bad)<br>(as determined by the<br>Clock Select Algorithm) |
|------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| *          | The Selected Time reference                                                                                                           | Truechimer                                                                                    |
| o          | The Selected PPS reference                                                                                                            | Truechimer                                                                                    |
| +          | A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected) | Truechimer                                                                                    |
| x          | "Falseticker" Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).                             | falseticker                                                                                   |
| -          | "Outlier" Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).                                 | falseticker                                                                                   |
| (blank)    | Source discarded: Failed Sanity check                                                                                                 | falseticker                                                                                   |

**Green: (SYNC):** NTP is in sync with this Peer/Server. NTP has either selected it as its reference or it's available for selection.

- Tally code is one of the following: \* or o or +
- Reach value is above 0

**Red (NOT IN SYNC):** This Peer/server is a falseticker. NTP hasn't selected it as its reference and it's NOT available for selection. The peer/server's time may be unreasonable, or it may not be in sync.

- Tally code is one of the following: x or - or blank
- Reach is above 0

**Orange (LIMITED REACH):** The Reach value of this Peer is not "177" but isn't "0" either. Either NTP was just restarted or not all Polls of that peer/server are resulting in a successful response. Packets may be getting lost in between, or that peer/server may not always be in sync and a useable reference (see below for additional troubleshooting info).

- Reach is above 0 but less than 177.
- See additional info directly below

**"Limited Reach" reported, though NTP wasn't just restarted in the last couple of minutes**

- Indicates not all Polls of a peer/server are resulting in a successful time response
- Displayed when the peer's/server's "Reach" value is greater than "0" but less than "177".

**Email Keith sent ( 4 Dec 2014)** Per our conversation, it looks like the Model 9489 may periodically be sending time requests to its two peers (the Model 9389s) but not always able to receive a response back from those time servers.

Limited Reach indicates that at least some, but not all, responses are being received. With a telnet or SSH connection, you can watch the Reach value counter to see when time responses aren't being received.

After logging in to the CLI interface, type the following command, which will automatically update every 2 seconds: `watch -n 1 ntpq -p`.

```
spadmin@Custservice ~$ watch -n 1 ntpq -p
```

```

spadmin@Custservice:~
Every 1.0s: ntpq -p Thu Dec 4 23:15:47 2014

remote refid st t when poll reach delay offset jitter

*PCI_TSYNC(0) .GPS. 0 1 4 16 377 0.000 0.006 0.002
oPPS(0) .PPS. 0 1 3 16 377 0.000 -0.008 0.002

```

This command will display and update the NTP statistics for each of NTP's references. The Poll value (in seconds) indicates how often NTP is currently sending NTP requests to that particular reference (at the beginning of the same row). The reach value will start at 0 when NTP first starts up and then increments at each Poll until it gets to "377". If it gets a response at each Poll of that reference, Reach will remain "377". But if one or more of the last 8 Polls doesn't result in NTP receiving a response from that peer, the Reach value decrements after the Poll occurred.

By the way, the "when" value is the number of seconds since it last sent a Poll to that time server. The Poll is sent when the "when" and "Poll" values are equal, with "when" becoming a vertical line instead of a number.

### Issue with one or more NTP peers disappearing (disappears from the list of configured peers)

- Sounds like this is an NTP bug in NTP v4.2.8p6 (software v5.4.1- expected fix to be in the v5.4.5 update)
- Refer to SR 5679 in SAP.

Q. (from Eric Bizimana) Everything seems to be working after the reboot but the peering to one of the other peers that disappeared again.

**A reply from Dave Lorah (11 Jul 16)** You will possibly see a NTP Peer disappear again. This is a bug in NTP software and can happen over and over. We are working on incorporating a fix by adding the new version NTP in the next Securesync firmware release.

---

### \*\*KHTD (KTS Host Time Daemon for Stratum 2 operation)

**Email from Dave Sohn (24 Apr 2014)** KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running.

### \*\*\*\*Dedicated NTP input- periodic Holdover alarms being asserted

- If NTP or KHTD are restarted for any reason while the unit remains up and running, SecureSync will go into Holdover mode (whether or not the Host clock driver, 127.127.45.0 is enabled). Holdover exits less than a minute or so later, once NTP/KHTD is back up and running.

### Log entry for KHTD being restarted

[system] KTS Host Time Daemon has restarted (KHTD)

### Log entries for NTPD being started/restarted

ntpd[31004]: ntpd 4.2.6p5@1.2349-o Fri Jan 30 15:51:28 UTC 2015 (1)

**Note:** this entry was with v5.2.0 installed (ntp 4.2.6). The NTP version is software version dependent (ntpd[31004]: ntpd 4.2 ....)

## Examples why either NTP or KHTD will be restarted include:

- NTP being restarted by a user
- NTP config change being made by a user (config changes automatically restart NTP)
- ntpdmon restating ntp due to a time error greater than one second

## Specific examples of Holdover alarms in a Stratum 2 server

### Kaiser Permanente

- Dedicated Stratum 2 SecureSync was periodically going into Holdover for less than a minute because NTP and KHTD were both restarting.

### Refer to Salesforce case 18014 for Kaiser Permanente

- Dedicated Stratum 2 SecureSync was periodically going into Holdover for a very short period of time (like a second or two). Then was fine again.
- Cause: "It appears that the network switch port for this unit was incorrectly configured and the eth0 interface was only operating at 10/half. It is now auto-negotiated to 100/Full and the problem seems to have gone away."

## KHTD restarting/Shutting down

- KHTD is restarted each time NTPD restarts

**Email from Paul Myers (24 Aug 2015)** If NTP is stopped and restarted KHTD will also be restarted. The NTP stop script 'reloads' KHTD to keep both at the same state.

## "KTS Host Time Daemon has terminated (KHTD)"

- This entry indicates NTP shutdown for halt/reboot by a user (other daemons will also be terminated, as well).

---

## ntpdmon: statistics logging (Client and server NTP packets per second- "pkt/s")

- Added this new NTP logging feature in software update version 5.2.1 (Apr 2015) as part of NTP v4.2.8 upgrade
- Entries are asserted into the NTP.log (NTP Log) each hour (27 minutes after each hour).
- Reports NTP loading
  - **Example log entry (with no clients):** NTP statistics: Clients = 0.000 pkt/s, Servers/Peers = 0.000 pkt/s
  - **Example log entry (with just a couple clients) NTP statistics:** Clients = 0.037 pkt/s, Servers/Peers = 0.000 pkt/s

### Where:

- **Clients:** NTP requests from NTP clients on the network
- **Servers/Peers:** NTP requests from Servers or Peers configured to get time from this SecureSync

## A) To convert pkt/s (values in the graphs/logs) to the actual number of packets in the hour

**Multiply** the number of pkt/s (value in the graphs/logs) **times 60** and then round-up to nearest whole number

### Examples:

**0.017 pkt/s = 1** packet in one hour

**0.083 pkt/s = 5** packets in one hour

0.167 pkt/s = 10 packets in one hour  
1.667 pkt/s = 100 packets in one hour  
166.667 pkt/s = 10,000 packets in one hour  
3000 pkt/s = 180,000 packets in one hour

## B) To convert actual number of packets per hour to pkt/s (values in the graphs/logs)

**Divide** the number of ntp packets in the hour by **60** (there are 60 minutes in the report period)

### Examples:

1 packet in one hour = **0.017 pkt/s**  
5 packets in one hour = **0.083 pkt/s**  
10 packets in one hour = **0.167 pkt/s**  
100 packets in one hour = **1.667 pkt/s**  
10,000 packets in one hour = **166.667 pkt/s**  
180,000 packets in one hour = **3000 pkt/s**

## NTP loading-NTP Throughput/NTP Statistics: Number of NTP requests per second/NTP Stress test

- Refer to: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP stress testing
- Refer to **NTP throughput documents on our website- links further below**
  - **SecureSync User Manual, generic note about throughput on page 10:** [http://spectracom.com/sites/default/files/document-files/SecureSync\\_UserRefGuide\\_1200-5000-0050\\_R21.pdf](http://spectracom.com/sites/default/files/document-files/SecureSync_UserRefGuide_1200-5000-0050_R21.pdf)
  - **Throughput (Q&A knowledge base article):** <http://support.spectracom.com/articles/FAQ/NTP-Throughput?&category=SecureSync&>
  - **Test protocol (tech note):** [http://spectracom.com/sites/default/files/document-files/NTP\\_Server\\_Capacity\\_Testing\\_TN19-101\\_B.pdf](http://spectracom.com/sites/default/files/document-files/NTP_Server_Capacity_Testing_TN19-101_B.pdf) (note this link is also available within the knowledge base article mentioned above)
- Refer to the [ntp.log](http://ntp.log) for info on NTP statistics (pkt/s)

## A) NTP statistics logging (Client and server NTP packets per second)

- Added this new NTP loading feature in software update version 5.2.1 (Apr 2015) as part of NTP v4.2.8 upgrade
- Provides NTP throughput / NTP loading
- Entries are asserted into the NTP.log (NTP Log)
  - **Example log entry (with no clients):** NTP statistics: Clients = 0.000 pkt/s, Servers/Peers = 0.000 pkt/s
  - **Example log entry (with just a couple clients) NTP statistics:** Clients = 0.037 pkt/s, Servers/Peers = 0.000 pkt/s

**Note:** pkt/s is reported in Mbps (Megabits/sec). So 0.140 pkt/s is 1400 packets per second ???

**Where:**

- **Clients:** NTP requests from NTP clients on the network
- **Servers/Peers:** NTP requests from Servers or Peers configured to get time from this SecureSync

**NTP throughput graphs added to web browser (versions 5.3.1 and above)**

- **Refer to:** NTP graphs

---

**NTP loading/NTP load testing/NTP throughput (By software version)**

**Published Spec used to be about 9309 packets/Sec.**

- Due to the ETX module changing from Intel to Realtec IC (and the associated change to a different driver) some time ago, the new spec is about 7500 requests/second on eth0. For eth1, eth2 and eth3, due to the faster port speed and different driver its around 8000 requests/second for these three ports

**Note:** Per Tom Richardson/Ron Dries, the SecureSyncs have never shipped with an ETX having an intel IC. The change to Realtec apparently occurred before we started shipping SecureSyncs and before we stopped shipping NetClock 9300s???

The info below in red (from email Keith sent on 15 Jun, 2016 after talking with Engineering/Hendrik) is regarding the newer ETX modules which have a Realtec (instead of Intel) component and therefore also a different driver for slightly lower numbers of responses/second. According to Tom R, this change to the ETX happened before we started shipping SecureSyncs???

Q. What is the max number of NTP requests per second?

**A. From Section 1.7.4 in the SecureSync manual, "Loading: ~7,000 NTP requests per second, typical"**

Q1. In the Manual version 20, this value is 9000, is it the correct value also for the latest unit? If no, please tell us the correct value.

**A Keith's response:** due to a hardware change, the NTP packets per second (NTP throughput) that the SecureSyncs can provide is now slightly lower than what was indicated in earlier versions of the SecureSync manual. Eth0 (the base 10/100 port installed on all SecureSyncs) can now provide about 7500 ntp requests/second.

As NTP intentionally staggers when each client polls its configured NTP servers, and as NTP doesn't request the time every second, these factors allows the SecureSync to be able to service WELL over 7500 NTP clients on its network.

The latest NTP throughput capability is indicated on page 10 of the latest version of the SecureSync manual, which can be downloaded at: [http://spectracom.com/sites/default/files/document-files/SecureSync\\_UserRefGuide\\_1200-5000-0050\\_R21.pdf](http://spectracom.com/sites/default/files/document-files/SecureSync_UserRefGuide_1200-5000-0050_R21.pdf) (the info is excerpted below for your convenience)

"NTP throughput: 7000 – 9000 NTP requests per second, depending on used Ethernet port/hardware configuration"

Note there is an available knowledge base article on website that also discusses throughput. It's available at: <http://support.spectracom.com/articles/FAQ/NTP-Throughput?&category=SecureSync&>

There is also a Tech Note/Test report referenced in the knowledge article mentioned above. here is the link to it: [http://spectracom.com/sites/default/files/document-files/NTP\\_Server\\_Capacity\\_Testing\\_TN19-101\\_B.pdf](http://spectracom.com/sites/default/files/document-files/NTP_Server_Capacity_Testing_TN19-101_B.pdf) (excerpt below):

The Spectracom NTP service implemented on SecureSync and NetClock 9400 was tested to determine its NTP



requests per second threshold value without authentication. Specific software components can affect throughput. An earlier configuration was capable of up to 9,909 NTP requests per second. An updated configuration was able to serve approximately 7,500 NTP requests per second.

Q2. If we use 1204-06 option module, does this value change?

**A Keith's response:** if one of the Ethernet interfaces on the Model 1204-06 Gb Ethernet Option Card (eth1, eth2 or eth3) is used instead of using eth0, the NTP loading capability for that one particular interface does increase slightly - due to the faster network speed of the interface and due to the Gb Ethernet interfaces using a different driver than eth0 uses. However, using more than one Ethernet interface on the SecureSync (eth0 through eth3) does not increase the overall number of NTP requests that the SecureSync can provide, as all of the Ethernet interfaces share the same instance of NTP.

So the number of NTP requests/second that NTP in the SecureSync can respond to is split amongst all Ethernet ports on the SecureSync which are receiving NTP requests (for example, if eth0 and eth1 are the only two Ethernet interfaces receiving NTP requests, eth 1 can be responding to 3500 request/sec while Eth0 is also responding to about 4000 requests- for a total of about 7500 NTP requests per second total being supplied by the SecureSync).

---

## A) Version 5.4.1

(17 Jun 2016) Summary of the info further below - per Ron Dries (based on testing with v5.4.1 I understand)

- Eth0 by itself (ETX module): ~7500 requests/sec
- Eth1, Eth2 or Eth3 by itself: ~8000-9000 requests/sec

---

## NTP load testing in more recent software versions (post 5.7.1.- with Spectre processing fixes added in 5.8.0?)

➤ Refer to Case 195013

### customer report

Having issues with v5.8.4 + patch 'updateGB3421.tar.gz', under NTP load testing.

The securesync has upstream STL device serving the securesync as NTP master & 1PPS. It has no direct GPS.

When sending NTP load testing the following occurs:

- Sending NTP 8000 req/sec device goes into Freerun (started at 13 may 9.20 UTC in logs).
- Loses its upstream NTP peer (i.e the STL).
- WEB GUI gets very very slow to respond.
- Cannot login via HTTP on chrome & cannot login thereafter (shows tacacs errors in log - the local spadmin username also does not work).
- However can login via HTTPS on chrome.
- However can login via HTTP on internet explorer.
- Device not allowing me to save & download logs from GUI.
  
- When sending NTP 3000 req/sec device does not go into Freerun but GUI unresponsive (started at 13 may 9.53 UTC in logs).

*Below in red is a report generated by the Apps team (based on their testing in the lab)*

Our Apps Team set up a similar configuration in our lab. Testing Stratum 2 performance with both STL and GPS as Stratum 1 reference under load of 8000-10,000 NTP requests per second. We did observe that under that significant load, the stratum 2 device would go into holdover as it was no longer able to receive information back from NTP. Any calls to query the NTP daemon for status time out - therefore we are not able to set the time into the timing system from NTP. Due to not being able to retrieve status from NTP the SecureSync goes into holdover. They confirmed that this is not related to the eth driver patch- that's working fine- and port flapping was not present. It appears directly related to the NTP overload. We spec a max of 7,000 NTP requests per second for SecureSync.

Regarding HTTP/HTTPS, when logging in through HTTPS then logging out - without closing your browser if you attempt

to log in with HTTP you will always be rejected. If you successfully logged in through HTTPS first, then later try HTTP, this will be the case. This can be fixed by closing your browser and reopening it, using a different browser/incognito, or clearing your cookies. SecureSync will be become slower to respond under that much NTP load.

Regarding your testing at 3000 req/sec- we did not observe any issues with lower load, I'm thinking this could be a symptom of the CF card failing

## **B) Version 5.9.4 (reported Feb 2022)**

### **Email from Gary Boff to Dave Lorah (28 Feb 2022)**

NTP Throughput testing was successfully tested with 5.9.4 using NTPStress.exe:

- NTP Throughput 5.9.4 **32-Bit** system: Avg Req/Sec = **7,698 (SOM-4455)**
- NTP Throughput 5.9.4 **64-Bit** system: Avg Req/Sec = **12,168 (SOM-4466)**

**Note for FYI** : SecureSync cut-in S/N for 64-Bit ETX (SOM-4466) was **17433** for commercial receivers and **ASD-1034** for SAASM receivers.

## **Load test reports (version installed not specified in test docs)**

<I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP stress testing\our NTP Stress test results\older versions of stress testing>

**2012: ~9909**

**2016: ~7500**

**2019: ~7500**

---

## NTP Stress Test tool (created by Spectracom Engineering)

- Refer to: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP stress testing

**Per Dave Sohn (6 Nov 15) customers do not need an NDA in place with us to receive this program. However, they need to be made aware of the following info**

**Email from Dave Sohn** We don't need an NDA in place, but they need to understand that this is an engineering tool we developed internally, so it is not a formally developed product with full support. It is provided as-is without any warranty.

**Note:** Don't send the entire contents of the "NTPStresTool" folder at the link above. Send the NtpStress.exe program, the "sample command.txt" document and this info (example I sent to a customer) I don't believe they need the "source" folder or the "StressTestTool.txt" file.

As this is an .exe that would most likely be "unattached" from this email (even if you actually received this email), I have uploaded it as a .zip file to the Sharefile website (a service we purchase for providing files). Both of you should have received a link to a folder containing this program. If you didn't get the link, please let me know!

Please be aware that this program is an engineering tool that our Engineers developed internally. So it is not a formally developed product with full support available. It is provided as-is without any warranties.

Accept

After pressing the above "Accept" button to agree to the terms mentioned 😊 , please feel free to use this program and Windows computers to generate MANY NTP time stamps!!

### DOS commands to run the tool

- Refer to the NTPStress sample command.txt document
- Tool can be run with the "COD" window left open or closed when the tool is run.

### Running the program

- 1) Open a command prompt window and change to the directory where ntpstress.exe is located.

```
C:\Users>e :
E:\>cd spectracom/ntpstress
```

- 2) Run the desired command (below):

### Syntax for single instance of the tool to run

**NtpStress.exe -t 10.10.128.85 10000 3600** where the IP address is the address of the NTP server, "10000" is the desired number of packets/sec for the tool to send ( note the actual number being sent may vary, such as far less based on capabilities of the PC) and "3600" is the number of seconds for the test to run.

### Syntax to automatically open/run more than one instance of the tool at the same time

**for /l %x in (1,1,10) do start cmd /k NtpStress.exe -t 10.10.128.85 10000 3600** (where the "10" -in red- is the number of instances to run at the same time. Also: where the IP address is the address of the NTP server, 10000 is the desired number of packets/sec for the tool to send (actual number may vary) and 3600 is the number of seconds for the test to run.

```

Attempting 1 NTP requests per second for 5 seconds from 10.10.128.85
Data will be written to "ntpdata.txt"
High performance frequency: 2630771
Will attempt to compensate for periodic time adjustments
Utilizing fine Sleep() measurement techniques
This test shall be finished by Fri Nov 13 17:48:30 2015
Pressing CTRL-C will terminate the data gathering and save the data.
1 NTP Req/Sec @ Second 00005 of the test

```

**Note:** the test can be ended at any time by pressing CTRL & C. Results below will be displayed.

### Results displayed when the test finishes

- How long it take the test to complete is based on the number of seconds specified in the last value of the command-such as “3600” seconds in the examples above )

```

1 NTP Req/Sec @ Second 00005 of the test
Generating Results file, please wait...Done!
Average NTP Req/Sec: 1
Total Requests: 4
Failed Requests: 0
Bad Stratum Level: 0

```

**Average NTP Req/Sec:** Average number of requests sent to the time server every second

**Total requests:** Total number of requests sent during the test duration.

**Failed requests:** Number of requests sent without a response from the NTP server.

**Bad Stratum level:** NTP Server was at stratum 16 when it responded (??)

## Manually stopping and restarting NTP

### Ability to enable/disable NTP via the CLI interface

Q. (Is there a way to enable NTP through the command line interface on SecureSync?)

A. Archive Version 4.8.9 added NTP (and SNMP) to the CLI “servget” and “servset” commands Starting with version 4.8.9, SNMP can be stopped or started using the servset command (SNMP status can be read using the servget command).

## NTPMOND (automatically restarts NTP)

- NTP Monitor daemon in the SecureSync used to automatically restart NTP if:
  - While it’s running, NTP exceeds sanity limit of 1000 seconds (16min 40 sec) with its reference - which can cause NTP to stop running.
  - In software versions 5.1.2 and above, NTPMOND will automatically restart NTP if NTP is in sync and the time error from KTS is 1 second or greater
- NTPMOND “wakes-up” and checks NTP every 16 seconds to check if NTP is running and if it’s within 1 second of the System Time (while synced to System Time)

**Note:** Per Ron Dries, NTPMOND “wakes-up” every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resyncs and be useable again.

## **NTP associated System logs for NTP being restarted (in the System log, not NTP log)**

```
[system] ntp monitor restarting ntpd (NTPMOND):
[system] ntp monitor stopping ntpd, found 3578 second difference followed by
[system] ntp monitor restarting ntpd (NTPMOND)
```

## **NTP.log entries also asserted:**

```
ntpd [xxxx] ntpd exiting on signal 15 followed by
ntpd [xxxx] "127.127.1.0 interface 127.0.0.1 -> (none)
```

**Note:** NTP also has its own Reference time change limits, as well (NTP step threshold)

- If NTP's selected input changes by **128 millisecond or less**, NTP **slews** to the reference
- If NTP's selected input changes by **more than 128 milliseconds** (and this error persists for more than the stepout threshold which has a default value of 900 seconds), NTP **steps** to the reference

## **Issue with NTPMOND trying to stop NTP when error >1 second**

- Version 5.3.0 update (~Sept 2015) fixed issue caused by NTP monitor Daemon (NTPMOND), trying to stop NTP when the Timing System and Linux kernel time differ by more than 1 sec

---

## NTP step threshold (NTP also has its own Reference time change limits, as well)

- If NTP's selected input changes by 128 milliseconds or less, NTP very slowly slews to the reference (maximum rate of 500 microseconds per second)
- If NTP's selected input changes by more than 128 milliseconds (and this error persists for more than the stepout threshold which has a default value of 900 seconds), NTP steps it's time to the reference ("Stepping means that the clock jumps abruptly from some incorrect time to some reasonable approximation of the correct time" - this is much faster than slewing).
- If the time error is greater than the panic threshold (1000 seconds which is 16 min 40 sec) NTP will stop syncing.

If the time error is less than 1000 seconds, but greater than the step threshold (128 ms) NTP starts a **900 second (by default) counter** . During this "wait", it's apparently verifying the information it's receiving is valid. At the end of 900 seconds (exactly 15 minutes) if the data was valid, NTP performs a "**Time Reset**" to the correct time (the NTP log will contain a "Time Reset" entry).

- To change the default duration of step threshold (shorter or longer) use the NTP Expert mode to add a "tinker stepout" line to the ntp.conf file. Example: Add "Tinker stepout 1800" to the ntp.conf file for a 30 minute wait before the time is corrected.

When first started, the daemon normally polls the servers listed in the configuration file at 64-s intervals. In order to allow a sufficient number of samples for the NTP algorithms to reliably discriminate between correctly operating servers and possible intruders, at least four valid messages from the majority of servers and peers listed in the configuration file is required before the daemon can set the local clock. However, if the difference between the client time and server time is greater than the panic threshold, which defaults to 1000 s, the daemon will send a message to the system log and shut down without setting the clock. It is necessary to set the local clock to within the panic threshold first, either manually by eyeball and wristwatch and the Unix `date` command, or by the `ntpdate` or `ntpd -q` commands. The panic threshold can be changed by the `tinker panic` command described on the [Miscellaneous Options](#) page. The panic threshold can be disabled entirely by the `-g` command line option described on the [ntpd - Network Time Protocol \(NTP\) daemon](#) page.

If the difference between local time and server time is less than the panic threshold but greater than the step threshold, which defaults to 128 ms, the daemon will perform a step adjustment; otherwise, it will gradually slew the clock to the nominal time. The step threshold can be changed by the `tinker step` command described on the [Miscellaneous Options](#) page. The step threshold can be disabled entirely by the `-x` command line option described on the [ntpd - Network Time Protocol \(NTP\) daemon](#) page. In this case the clock will never be stepped; however, users should understand the implications for doing this in a distributed data network where all processing must be tightly synchronized. See the [NTP Timescale and Leap Seconds](#) page for further information. If a step adjustment is made, the clock discipline algorithm will start all over again, requiring another round of at least four messages as before. This is necessary so that all servers and peers operate on the same set of time values.

The clock discipline algorithm is designed to avoid large noise spikes that might occur on a congested network or access line. If an offset sample exceeds the step threshold, it is ignored and a timer started. If a later sample is below the step threshold, the counter is reset. However, if the counter is greater than the stepout interval, which defaults to 900 s, the next sample will step or slew the time as directed. The stepout threshold can be changed by the `tinker stepout` command described on the [Miscellaneous Options](#) page.

---

## “View NTP Clients” (NTP “Monlist”, “MRU list”, NTP client list)

- This capability started in Archive software version 5.1.2.
- Can view up to the last **600** NTP clients (both monlist and mrulist)
- table info can be viewed in the web browser or via the CLI interface

Refer to online SecureSync user guide at:

[http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_ClientsViewing.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_ClientsViewing.htm)

**Excerpt of email from Keith (10 Sept 2018, for at least 5.8.1 and below)**

### **View NTP Clients” table**

Note that NTP also provides SecureSync with an NTP Clients list, which works well if there are less than **600** clients on the network. If there are more than 600 NTP Clients configured to sync to a SecureSync/Sync, we **do not** recommend viewing this NTP Clients data table, as the entries in the table are rotated out too quickly to be helpful.

If there are more than **600** NTP clients on the network and you wish to see which NTP clients are syncing to it, we recommend using a wireshark/tcpdump packet capture to view all NTP (port 123) packets having a “**destination**” IP address being the same as the SecureSync’s IP address. This packet capture will show network nodes sending NTP requests to the SecureSync

### **A) mrulist (Most Recently Used) (versions 5.2.1 and above)**

Refer to <https://www.eecis.udel.edu/~mills/ntp/html/miscopt.html>

#### **mindepth count**

Lower limit on the MRU list size. When the MRU list has fewer than mindepth entries, existing entries are never removed to make room for newer ones, regardless of their age. **The default is 600 entries.**

- Available in the **Management** -> **NTP Setup** page of the browser. Click on the “**View NTP clients**” button in the upper-left corner of the page.
- Results are obtained from either an internal NTPQ mrulist query (v5.2.1 and above) or from an internal NTPDC monlist query (v5.2.0 and below)
- “MRU” stands for “Most Recently Used”
- This table can also be viewed via the CLI interface. See details further below for which CLI command to perform, based on version of software installed.

**Note:** This table **does not list other NTP Peers/Servers that are getting time from this NTP server, just NTP clients**

The screenshot shows the 'NTP Clients' interface. A table displays client information with the following data:

| Client IP   | Received Packets | Mode | Version | Restriction Flags | Avg Interval | Last Interval |
|-------------|------------------|------|---------|-------------------|--------------|---------------|
| 10.2.100.42 | 60               | 3    | 4       | c0                | 17           | 8             |
| 10.2.100.87 | 8                | 3    | 4       | c0                | 115          | 28            |

Callouts in the image explain the fields: 'Packets received since NTP first started up' points to the 'Received Packets' column; 'Average interval in Seconds between packets' points to the 'Avg Interval' column; 'Seconds since last received packet' points to the 'Last Interval' column. A search bar is visible at the top right, and navigation buttons (First, Previous, 1, Next, Last) are at the bottom right. A red arrow points to the 'View NTP Clients' menu item on the left sidebar.

**Per the online SecureSync user guide**

**View NTP Clients:** Click here to reveal a table of all the clients your SecureSync is servicing. (See also [Viewing NTP Clients.](#)) Information for each client includes:

- Client IP
- Received Packets
- Mode
- Version
- Restriction Flags
- Avg Interval
- Last Interval

**Refresh/update of the displayed data in this table**

- Refer to Mantis case 3164
- As observed in v5.3.0- the data in the table is only updated when this pop-up window is closed /re-opened
  - If the table/pop-up window remains open, the data doesn't update.

**Description of fields**

- From: <http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html#mrulist> (listed in opposite order as the table)



order. The output columns are:

| Column                      | Description                                                                                                                                                                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>lrint</code>          | Interval in s between the receipt of the most recent packet from this address and the completion of the retrieval of the MRU list by <code>ntpq</code> .                                                                                                        |
| <code>avgint</code>         | Average interval in s between packets from this address.                                                                                                                                                                                                        |
| <code>rstr</code>           | Restriction flags associated with this address. Most are copied unchanged from the matching <code>restrict</code> command, however 0x400 (kod) and 0x20 (limited) flags are cleared unless the last packet from this address triggered a rate control response. |
| <code>r</code>              | Rate control indicator, either a period, <code>L</code> or <code>K</code> for no rate control response, rate limiting by discarding, or rate limiting with a KoD response, respectively.                                                                        |
| <code>m</code>              | Packet mode.                                                                                                                                                                                                                                                    |
| <code>v</code>              | Packet version number.                                                                                                                                                                                                                                          |
| <code>count</code>          | Packets received from this address.                                                                                                                                                                                                                             |
| <code>rport</code>          | Source port of last packet from this address.                                                                                                                                                                                                                   |
| <code>remote address</code> | DNS name, numeric address, or address followed by claimed DNS name which could not be verified in parentheses.                                                                                                                                                  |

## B) NTP Mode (Packet Mode):

**Note:** Modes are excerpted below from <http://lists.ntp.org/pipermail/questions/2007-February/013070.html>

'm'ode is the mode seen in the packet from the remote address/port, defined in `ntp.h`:

```
MODE_UNSPEC 0 /* unspecified (old version) */
MODE_ACTIVE 1 /* symmetric active mode */
MODE_PASSIVE 2 /* symmetric passive mode */
MODE_CLIENT 3 /* client mode */
MODE_SERVER 4 /* server mode */
MODE_BROADCAST 5 /* broadcast mode */
MODE_CONTROL 6 /* control mode [ntpq] */
MODE_PRIVATE 7 /* private mode [ntpd] */
```

## C) Restriction Flags ("RSTR" Column)

- Codes are from <http://lists.ntp.org/pipermail/questions/2007-February/013070.html>

| Restriction<br>Flags | A |
|----------------------|---|
| c0                   | 1 |

| Code "c"                                                                  | NTP Restrict Flag              | Description (see full descriptions in table further below)                                              |
|---------------------------------------------------------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------|
| Individual flags                                                          |                                |                                                                                                         |
| c0                                                                        |                                | No restrict flags                                                                                       |
| c1                                                                        | ignore                         | ignore packet                                                                                           |
| c2                                                                        | noserve                        | access denied                                                                                           |
| c4                                                                        | notrust                        | authentication required                                                                                 |
| c8                                                                        | version                        | version mismatch                                                                                        |
| c10                                                                       | nopeer                         | new association denied                                                                                  |
| c20                                                                       | limited                        | packet rate exceeded                                                                                    |
| c40                                                                       | noquery                        | mode 6/7 packet denied                                                                                  |
| c80                                                                       | nomodify                       | mode 6/7 modify denied                                                                                  |
| c100                                                                      | notrap                         | mode 6/7 set trap denied                                                                                |
| c200                                                                      | lptrap                         | mode 6/7 low priority trap                                                                              |
| c400                                                                      | demobilize                     | send kiss of death packet                                                                               |
| c800                                                                      | timeout                        | timeout this entry                                                                                      |
| Combinations of flags (start with largest possible code and then go down) |                                |                                                                                                         |
| 194                                                                       | notrap+nomodify+nopeer+notrust | mode 6/7 set trap denied<br>mode 6/7 modify denied<br>new association denied<br>authentication required |

The **nomodify** options prevents any changes to the NTP configuration.

The **notrap** option prevents ntpdc control message protocol traps.

Per the website: <http://lists.ntp.org/pipermail/questions/2007-February/013070.html>, Restriction Fags can use a single number to represent more than one value (the numbers for the various states are additive).

code' is a hex value made up of flag bits from the entry matching the remote address in the restrict list (ntpdc -nc reslist), again defined in ntp.h:

```
RES_IGNORE 0x001 /* ignore packet */
RES_DONTSERVE 0x002 /* access denied */
RES_DONTTRUST 0x004 /* authentication required */
RES_VERSION 0x008 /* version mismatch */
RES_NOPEER 0x010 /* new association denied */
RES_LIMITED 0x020 /* packet rate exceeded */
RES_NOQUERY 0x040 /* mode 6/7 packet denied */
RES_NOMODIFY 0x080 /* mode 6/7 modify denied */
RES_NOTRAP 0x100 /* mode 6/7 set trap denied */
RES_LPTRAP 0x200 /* mode 6/7 low priority trap */
RES_DEMOBILIZE 0x400 /* send kiss of death packet */
RES_TIMEOUT 0x800 /* timeout this entry */
```

For instance, c180 is a combination of both 100 and 80 (you start with the largest available value first, and the remainder is either one value, or more than one value).

100 and 80 are the factory default values indicating NTP is configured for No Modify and no Trap. (No Modify means NTPQ on another NTP machine cant remotely make changes to the NTP settings inside the SecureSync. Not sure

about noTrap).

From: <http://www.eecis.udel.edu/~mills/ntp/html/accopt.html#limited>

Some flags have the effect to deny service, some have the effect to enable service and some are conditioned by other flags. The flags are not orthogonal, in that more restrictive flags will often make less restrictive ones redundant. The flags that deny service are classed in two categories, those that restrict time service and those that restrict informational queries and attempts to do run-time reconfiguration of the server. One or more of the following flags may be specified:

**flake**  
Discard received NTP packets with probability 0.1; that is, on average drop one packet in ten. This is for testing and amusement. The name comes from Bob Braden's *flakeway*, which once did a similar thing for early internet testing.

**ignore**  
Deny packets of all kinds, including `ntpq` and `ntpd` queries.

**kod**  
Send a kiss-o'-death (KoD) packet if the `limited` flag is present and a packet violates the rate limits established by the `discard` command. KoD packets are themselves rate limited for each source address separately. If the `kod` flag is used in a restriction which does not have the `limited` flag, no KoD responses will result.

**limited**  
Deny time service if the packet violates the rate limits established by the `discard` command. This does not apply to `ntpq` and `ntpd` queries.

**lowpriotrap**  
Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first served basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps.

**msntp**  
Enable Microsoft Windows MS-SNTP authentication using Active Directory services. Note: Potential users should be aware that these services involve a TCP connection to another process that could potentially block, denying services to other users. Therefore, this flag should be used only for a dedicated server with no clients other than MS-SNTP.

**nomodify**  
Deny `ntpq` and `ntpd` queries which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

**noquery**  
Deny `ntpq` and `ntpd` queries. Time service is not affected.

**nopeer**  
Deny packets that might mobilize an association unless authenticated. This includes broadcast, symmetric-active and multicast server packets when a configured association does not exist. Note that this flag does not apply to packets that do not attempt to mobilize an association.

**noserve**  
Deny all packets except `ntpq` and `ntpd` queries.

**notrap**  
Decline to provide mode 6 control message trap service to matching hosts. The trap service is a subsystem of the `ntpd` control message protocol which is intended for use by remote event logging programs.

**notrust**  
Deny packets that are not cryptographically authenticated. Note carefully how this flag interacts with the `auth` option of the `enable` and `disable` commands. If `auth` is enabled, which is the default, authentication is required for all packets that might mobilize an association. If `auth` is disabled, but the `notrust` flag is not present, an association can be mobilized whether or not authenticated. If `auth` is disabled, but the `notrust` flag is present, authentication is required only for the specified address/mask range.

**ntpport**  
This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). A restrict line containing `ntpport` is considered more specific than one with the same address and mask, but lacking `ntpport`.

**version**  
Deny packets that do not match the current NTP version.

(from <http://support.ntp.org/bin/view/Support/AccessRestrictions>)

### 6.5.2. Access Control Options

There are numerous Access Control options which may be used on the restrict lines in your `ntp.conf`. Some of the more commonly used options are described in detail here.

- **nomodify** -- "Do not allow this host/subnet to modify the **ntpd** settings **even if they have the correct keys.**" By default `ntpd` requires authentication with symmetric keys for modifications made with `ntpd`. So if you don't configure symmetric keys for your `ntpd`, or keep them properly safeguarded, you don't need to use 'nomodify' unless you are concerned that the NTP authentication scheme might be compromised.
- **noserve** -- "Do not serve time to this host/subnet." This option is really intended to be used when you want to allow a host/subnet to access your `ntpd` only for monitoring and/or remote configuration.

- **notrust** -- "Ignore all NTP packets that are not cryptographically authenticated." This option tells ntpd to ignore all packets which are not cryptographically authenticated (note that this is a change from ntp-4.1.x). DO NOT use "notrust" unless ntp crypto (i.e. symmetric keys or autokey) has been properly configured on "both ends" of an ntp association (e.g. your ntpd and a remote time server, your ntpd and a client). See [6.5.3.1. notrust changed between versions 4.1 and 4.2](#) for more information.
- **noquery** -- "Do not allow this host/subnet to query your ntpd status." The ntpd status query features provided by ntpq/ntpdc will reveal some information about the system running ntpd (e.g. OS version, ntpd version) that you may not wish others to know. You need to decide if concealing this information is more important than the possible benefits of allowing your clients to see synchronization information about your ntpd.

### Desire to modify the functionality of the NTP Clients list

**Email from Dave Sohn** We utilize the standard ntp package in our underlying system. With this package we are able to see its current view of the client list. This information is not monitored in real-time by the system, and is queried on an as-needed basis. We do not have notifications or alarming of added or dropped clients in the client list. We also do not have the ability to clear older entries out of the list on demand.

- The data for this table is grabbed directly from NTP. We do not have the capability to modify the functionality of the mrulist or monlist commands.

### Desire to reset the monlist table

- Engineering confirmed the only ways to reset the table (whether viewing it in the browser or via the CLI interface command) is to stop/start NTP or reboot the time server.

### Additional info on NTP clients list

**Email from Dave Lorah (3 Aug 2015)** I was able to get some more information on the operation of the NTP Clients table in the 9483.

1) The clients are entered in the order received. This list reports the NTP clients (up to about 600 NTP clients maximum. Note this table **does not list other NTP Peers that are getting time from this NTP server, just NTP clients**) that have requested time stamps, how many NTP requests each client has sent to this time server and how often each client is sending a time request.

2) The table is limited in monitoring current status of an NTP Client. It will only show the number of packets received, and the last interval (time since last request) to show if an NTP Client is active. Check if the Received Packets are incrementing to see if a certain NTP Client is still active.

3) The table can be reset by turning NTP Off/ON or rebooting the 9483. It will then start accumulating NTP Clients again.

The search field at the top of the window allows you to be able to search to see if a particular client is in this list. It searches for "any part" of the field). If the NTP client hasn't requested time from this NTP server yet or is not configured to get time from this NTP server, the search field will return the following message shown below ("**No matching records found**")

After firmware version 5.1.7 the NTP Monlist was removed from the firmware due to security vulnerability issues. At this time the NTP Client list in the web browser is the only method for identifying NTP Clients.

### Determining if a client has stopped polling the time server without resetting the table

*Watch the "Received Packets" field to see if it's still incrementing. Other fields will continue to increment if a client goes away. But this field will stop incrementing until it starts polling again.*

**(email Keith sent to a customer, 29 Aug 2014)** Regarding your earlier questions about NTP's ability to report what NTP clients are polling the time server via the SecureSync's web browser, an engineer confirmed our belief that the only way to clear/reset this table is to stop and restart NTP using the browser (or by rebooting the time server).

However, in lieu of restarting NTP, you can periodically monitor the “Received Packets” column to see if it’s still incrementing. If this value increments, the client is still sending time requests to the time server. But if this value remains constant, the time server is no longer receiving packets from this client. The minpoll and maxpoll intervals of NTP in the client will determine how often this value should be incrementing for a particular client. If the maxpoll interval has elapsed without this field incrementing, the server did not receive a time request from that client.

**Known NTP issue if pressing the “View NTP Clients” button if there are more than 600 NTP clients pointing to the time server.**

- error.log has entries regarding “MRU” (two example entries below)

Giving up after 8 restarts from the beginning.

With high-traffic NTP servers, this can occur if the MRU list is limited to less than about 16 seconds' of entries. See the 'mru' ntp.conf directive to adjust.

**Ctrl-C will stop MRU retrieval and display partial results.**

- Can cause “crashing” of web browser? And/or “out of memory manager” entries in kern.log?

**\*\*Desire to view the “NTP client list” info using CLI interface**

**A) Versions 5.2.1 and above (using the mrulist command)**

- **Note:** can also “watch” the table update, if desired. See modified command further below)

**ntpq -c mrulist**

```
ntpq> exit
spadmin@CustService-176 ~ $ ntpq -c mrulist
Ctrl-C will stop MRU retrieval and display partial results.
Retrieved 3 unique MRU entries and 0 updates.
lstint avgint rstr r m v count rport remote address

5 4 c0 . 3 4 16002 123 10.2.100.177
8 64 c0 . 3 4 993 123 10.2.100.124
51 65 c0 . 3 4 963 123 10.2.100.95
```

**To watch the mrulist table automatically refresh once-per-second:**

```
spadmin@CustService-176 ~ $ watch -n1 ntpq -c mrulist
```

**watch -n1 ntpq -c mrulist**

**B) NTPC (Versions 5.2.0 and below-before NTPDC was replaced by NTPQ in NTP)**

**Note:** can also “watch” it update, if desired)

```
spectracom NetClock 9483 Version 5.1.5
spadmin@Spectracom ~ $ ntpdc -n -c monlist
remote address port local address count m ver rstr avgint lstint

10.2.100.177 123 10.2.100.176 44 1 4 c0 15 9
10.2.100.87 123 10.2.100.176 1 3 4 c0 35 35
10.2.100.140 65005 10.2.100.176 14 3 4 c0 48 47
10.10.128.32 123 10.2.100.176 1 3 4 c0 449 449
```

**To watch the table automatically update once per second:**

```
spadmin@Spectracom ~ $ watch -n 1 ntpdc -n -c monlist
```

## \*\*Desire to output the “NTP client list” info using the REST API interface

- Refer to Salesforce cases such as 289754

## \*\*Desire to output NTP in Local Time (instead of NTP)

- Refer to Salesforce case 15042
- Requires all external input references be removed/disabled in the Reference Priority table
- System Time is set to “local time” instead of UTC
- No automatic DST correction (System Time needs to be manually changed every 6 months)

**Email from Dave Lorah (20 Jun 14)** I did some research and experimentation and have the following instructions to setup your SecureSync unit to transmit local time zone from NTP. This involves setting up a Reference Priority Table entry and then manually setting the SecureSync time to your local time.

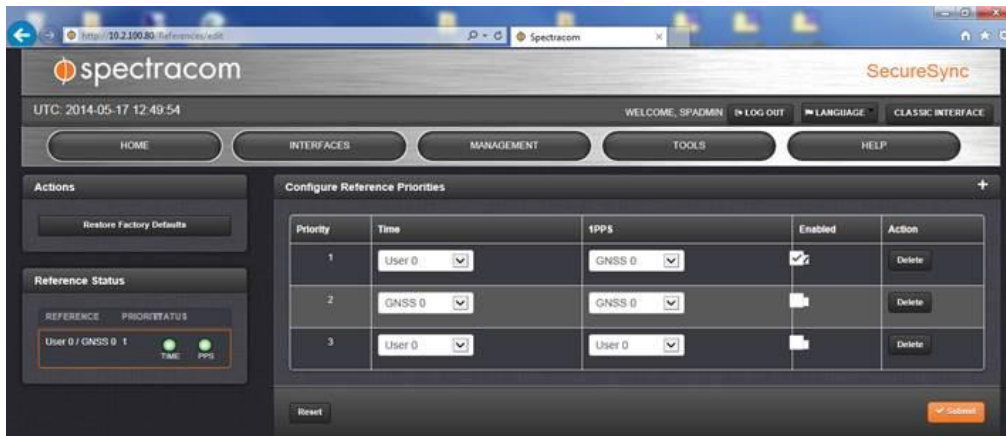
There is no way possible to introduce a Daylight Savings Time offset schedule, however. So, you will need to go into the unit and manually set the time twice a year to correct the DST offset.

You should update to current version 5.1.4 to eliminate the NTP 1000mS correction limitation. Here is a link to the download:

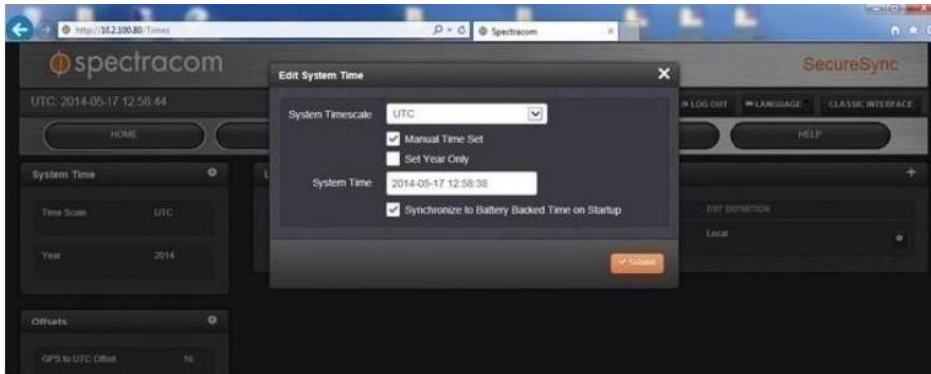
<http://www.spectracomcorp.com/Support/HowCanWeHelpYou/SoftwareUpdates/SecureSyncSoftware/tabid/1352/Default.aspx>

### Setup Procedure:

1. Create a Reference Priority Table entry for **User0 / GNSS 0**.



2. Next, go to the **Management -> Time Management** section and select the System Time config. Select the “**Synchronize to Battery Backed Time on Startup**” checkbox. Also select the “**Manual Time Set**” checkbox.
3. Enter your local time in the System Time field. When you hit SUBMIT it will manually set the system time and start running from there. When DST goes into effect you will have to go back to this same page and change the time manually as needed.
4. The SecureSync will start running from this manually set time and keep precisely running using the GPS 1PPS as a reference.



## Desire to prevent NTP from responding to earlier versions NTP requests (NTPv1, NTPv2 and NTPv3. Responding to NTPv4 requests only)

- Refer to “version” in the following link <http://www.manpagez.com/man/5/ntp.conf/> (under “Access Control Support”)
- Refer to the NTP Expert Tech Note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert mode- restrict earlier versions

Q. ST Electronics (Info-Security) wants to know if SS can be disabled for NTPv1 and v2. They want to restrict the unit to serve only NTPv3 and v4 requests. They currently have 3 RB SS at the staging area but will need an official response from Spectracom.

A This was a great question. We don't recall anyone EVER asking for this capability before.

NTP doesn't appear to support exactly what they want to do, but it can come VERY close. The SecureSyncs don't directly support this function of NTP with browser fields, but it can be implemented with the NTP Expert mode.

NTP has an access restriction flag available that will block all NTP requests that are not from clients at the same version of NTP it is running. So, the only difference with what your customer desires and what NTP can do is it will block V1, v2 and v3 requests, allowing only v4 requests to be responded to. It doesn't allow you to specify which versions are allowed and which versions aren't allowed. As this is the only customer ever to ask for this capability, I suspect it won't be added to directly to a field in the browser in any future release (it will be limited to just the Expert Mode).

If your customer would like to allow only v4 requests be responded to, here is how to configure this using the Expert Mode. Note that Expert Mode needs to remain always enabled once it's manually changed. Disabling Expert mode will cause any changes to be lost as the ntp.conf file is reset back to the factory default state. While enabled, the majority of the NTP configurations fields will no longer be visible. But NTP can be enabled or disabled if desired, without needing to disable Expert Mode.

- 1) Go to the Management -> NTP Setup page
- 2) On the left side of the page, change Expert Mode to ON
- 3) Click on the Gear ICON just above the NTP switch and next to the right of “NTP Services”, This will open the “Expert Mode” Window, as shown below:



- 4) With the window open, add the word “version” to the end of the third and fourth lines in this window (after the

word “nomodify”, as shown above). This will restrict NTP responses to only version 4 clients, via either IPv4 or IPv6 addresses!

---

## NTP IPv4/IPv6 Access Restriction / NTPQ and NTPDC (Mode 7)

- Refer to the Knowledge base article on our website:
- For more info, refer to: <http://support.ntp.org/bin/view/Support/AccessRestrictions>

### NTP access restriction configuration (via Expert mode, the newer web browser or classic interface)

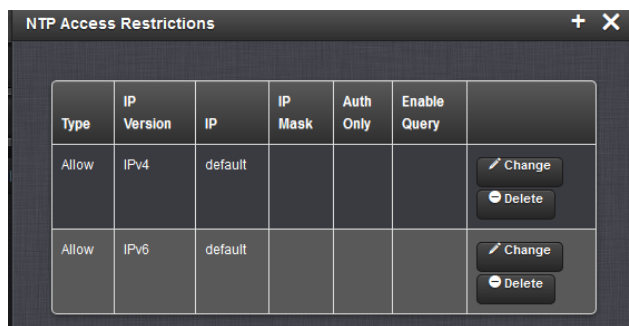
#### NTP Expert mode enabled

- Refer to Section 6.5.1 of the following link for info on how to edit the ntp.conf file directly for NTP access restrictions: <http://support.ntp.org/bin/view/Support/AccessRestrictions>
- Note when NTP Expert mode is enabled, the change/delete buttons in the NTP Access Restrictions table are not disabled, to prevent editing the settings via the web browser instead of editing the ntp.conf file.

#### A) Newer (black/charcoal) browser:

- NTP Access Restriction and Mode 7 (NTPQ and NTPDC) are both configured in the **Management -> NTP Setup** page of the browser. Click on the Access Restrictions button on the left side of the page.

##### Factory default settings



| Type  | IP Version | IP      | IP Mask | Auth Only | Enable Query |                                                                                |
|-------|------------|---------|---------|-----------|--------------|--------------------------------------------------------------------------------|
| Allow | IPv4       | default |         |           |              | <input type="button" value="Change"/><br><input type="button" value="Delete"/> |
| Allow | IPv6       | default |         |           |              | <input type="button" value="Change"/><br><input type="button" value="Delete"/> |

#### B) Classic interface:

- NTP Access Restriction and Mode 7 (NTPQ and NTPDC) are both configured in the Network -> NTP Setup page of the browser, NTP Access tab

### Summary: To allow only one or only some NTP clients to get time from the SecureSync

- In order to “allow” just one or more NTP clients to have access, you first have to “Deny” all clients. Then, if you want to:
  - 1) Allow individual clients (not an entire subnet), you add individual rows in the table that define the IP address – with no subnet mask defined.
  - 2) Add additional rows of IP address only for each additional client you wish to Allow (no subnet mask).
  - 3) Allow an entire subnet (not just one particular client) define the IP address of one client on that subnet and also enter the subnet mask for the network you wish to allow.

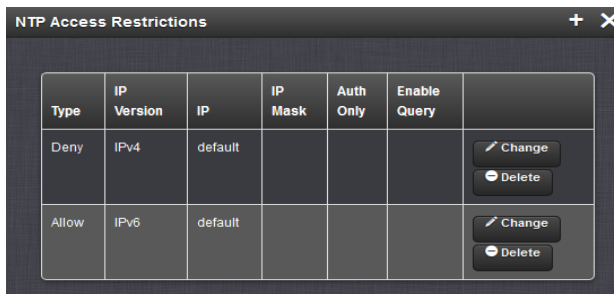
#### C) Specific steps to configure one or more NTP clients to be able to access the time server:

1. First “Deny” access to every client on the IPv4 network:



A) In the first row of the Access table (IPv4) just press “Change” and then switch “Allow” to “Deny”.

B) Press Submit.



| Type  | IP Version | IP      | IP Mask | Auth Only | Enable Query |                                                                                |
|-------|------------|---------|---------|-----------|--------------|--------------------------------------------------------------------------------|
| Deny  | IPv4       | default |         |           |              | <input type="button" value="Change"/><br><input type="button" value="Delete"/> |
| Allow | IPv6       | default |         |           |              | <input type="button" value="Change"/><br><input type="button" value="Delete"/> |

2. Then add an “Allow” for each client that you want to be able to access NTP from this time server:

A) Enter just the IP address and no subnet mask to allow just an individual client. Continue entering new “Allow” IP address lines to allow additional clients.

B) Enter an IP address and subnet mask (such as 10.2.1.2 255.255.0.0) to allow that entire subnet to have access. In this example, all clients on the 10.2.x.x network can get time from the server.

**Note:** can’t enter just enter a subnet with no associated IP address.

3. Press the “+” to add a client or subnet to allow



NTP Access Restrictions

Restriction Type:

IP Version:

IP Address:

Subnet Mask:

Require Authentication:

Allow NTP Control:

4. Restriction Type: Select “Allow”

5. IP Address: enter a desired client to Allow, or any client on the subnet that is desired to be allowed.



NTP Access Restrictions

Restriction Type:

IP Version:

IP Address:

Subnet Mask:

Require Authentication:

Allow NTP Control:

6. Subnet mask: enter ONLY if it’s desired to Allow that entire subnet.



NTP Access Restrictions

Restriction Type:

IP Version:

IP Address:

Subnet Mask:

Require Authentication:

Allow NTP Control:

7. Press Submit.

First, all NTP clients are Denied

Then, only one NTP client is allowed (additional lines can be added to allow other NTP clients)

| Type  | IP Version | IP          | IP Mask | Auth Only | Enable Query |                  |
|-------|------------|-------------|---------|-----------|--------------|------------------|
| Deny  | IPv4       | default     |         |           |              | Change<br>Delete |
| Allow | IPv6       | default     |         |           |              | Change<br>Delete |
| Allow |            | 192.168.1.* |         | 0         | 0            | Change<br>Delete |

Now ONLY **192.168.1.2** can now access the server. All other clients are denied.

**D) Repeat Step “C” for each additional client you wish to allow access to the time server**

---

## NTPv6 Access Restriction

### Issue with at least software versions 5.1.5 and below

- Refer to Mantis case 2910

**Email Keith sent (23 Sept 14)** Per your inquiry “system configured with access restriction to allow queries from 2607:b400:0000:: with mask of ffff:ffff:ff00:: ntpdc -c reslist returns line with incorrect mask and system cannot be queried from a matching remote system. reslist returns: 2607:b400:: ffff:ffff:ffff: 0 none”, I have some information for you that I hope will help.

This IPv6 configuration of the SecureSync currently requires the use of the available NTP Expert Mode functionality. Once NTP has been reconfigured in the web browser for Expert mode, the raw ntp.conf file can be edited with a “-6” being added to this file. Once this value has been enabled. NTP Expert Mode will need to remain enabled for the change to persist.

NTP access restrictions are discussed in the following document:  
<http://support.ntp.org/bin/view/Support/AccessRestrictions>

I am also passing this information over to our Product Management and Engineering teams for consideration of adding this capability in a future update to alleviate needing to use the Expert mode to configure it for IPv6.

### Configuring NTP Expert mode:

With other desired configuration changes to the default NTP pages of the browser already set as desired, enable the Expert mode (note the browser fields aren't accessible once NTP expert mode is enabled). And if Expert mode is subsequently disabled, this file will return to its default state. So Expert Mode needs to remain enabled to keep the settings.

To enable Expert mode with software versions 5.1.2 and higher installed via the newer web browser, go to the **Management -> NTP Setup** page of the browser. On the left side of this page, slide the “Expert Mode” slider bar over to the ON. This will open a pop-up menu displaying the raw ntp.conf file. The document referenced above will discuss how to edit this configuration file for your IPv6 requirements.

### Follow-up email Keith sent to this customer.

There are two changes we recommend you incorporate in the ntp.conf file edits you are adding:

- 1) restrict ::1 should be changed to: restrict -6 ::1
- 2) you should remove: restrict -4 default ignore (It's not needed)

So the new code with these two changes incorporated should now look like the following:

```
restrict 127.0.0.1
restrict -6 ::1
restrict -6 default nomodify noquery
```

## NTPQ (Mode 6) and NTPDC (Mode 7)

### NTPQ (Mode 6)

- The ntpq utility program is used to monitor NTP daemon ntpd operations and determine performance.
- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html> And <http://ftp.netbsd.org/pub/NetBSD/NetBSD-current/src/external/bsd/ntp/dist/ntpq/ntpq.html#System-Variables> (ntpq user's manual)

### Confirming mode 6 queries are still disabled

- Refer to Salesforce Case 178716

### Your question

We have a Spectracom SecureSync, Model 1200-213 (serial 13871). We have an open audit ticket to restrict Mode 6 queries. Could you please let me know where in the configuration I should modify to keep the until from responding to such queries?

### My response

In summary of the info below, Mode 6 queries are disabled by factory default. Unless a user has since enabled the NTP queries, Mode 6 queries are already being blocked.

In case you weren't already aware, there is a great (very easy searchable) online SecureSync user guide. This document contains the most current info about the SecureSync.

For verifying Mode 6 queries is still disabled, refer to "**allow NTP queries**" at the very bottom of the following page: [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/NTP\\_AccsRestrict.htm?Highlight=ntp%20queries](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/NTP_AccsRestrict.htm?Highlight=ntp%20queries)

And, press the "**Access Restrictions**" button on left side of the **Management -> NTP Setup** page of the browser. This will open a pop-up window. as shown below, Mode 6 queries are still disabled if the "**Enable Query**" boxes (for IPv4 and IPv6) are both empty:



### NTPDC (Mode 7)

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/ntpdc.html>
  - The ntpdc is used to **query the ntpd daemon about its current state** and to request changes in that state.
  - NTPDC no longer available
  - NTPDC is being removed with the NTP version 4.2.8 update (Software version 5.2.1, ~May 8<sup>th</sup>). It was removed from NTP in this newer version of NTP. NTPQ is still available in NTP 4.2.8.

### Desire to use Mode 7 queries

- If it's desired to enable Mode 7 queries from anywhere on the network, select the "Allow queries from NTPDC or NTPQ over IPv4" and/or the "Allow queries from NTPDC or NTPQ over IPv6" checkboxes (as applicable) at the top of the "NTP Access" tab.

- If there are custom entries added in the Access table (below the list of checkboxes) and its desired to enable NTPQ/NTPDC, uncheck the Allow queries from NTPDC or NTPQ over IPv4” and “Allow queries from NTPDC or NTPQ over IPv6” checkboxes at the top of this NTP Access tab, and select the individual “Enable Query” checkboxes in the last column of the NTP Access table. These individual checkboxes override the two “Allow queries...” checkboxes at the top of this tab.

## NTPQ (Mode 6) /NTPDC (Mode 7)

### Desire to use Mode 6/ Mode 7 queries

- Mode 7 queries no longer available starting with NTP version 4.2.8p2 (software versions 5.2.1 and above).
- If it’s desired to enable Mode 6 and 7 queries from anywhere on the network, select the “Allow queries from NTPDC or NTPQ over IPv4” and/or the “Allow queries from NTPDC or NTPQ over IPv6” checkboxes (as applicable) at the top of the “NTP Access” tab.
- If there are custom entries added in the Access table (below the list of checkboxes) and its desired to enable NTPQ/NTPDC, uncheck the Allow queries from NTPDC or NTPQ over IPv4” and “Allow queries from NTPDC or NTPQ over IPv6” checkboxes at the top of this NTP Access tab, and select the individual “Enable Query” checkboxes in the last column of the NTP Access table. These individual checkboxes override the two “Allow queries...” checkboxes at the top of this tab.

### Reported Issue: ShadowServer is reporting NTP is responding to Mode 6 requests, even though “NTP Queries” is disabled in NTP Setup page

- Refer to Salesforce case 25589 (9 Jun 17)
- Refer also to
- With v5.5.1 installed, Nessus scanner reported NetClock is responding to Mode 6 queries even though queries are not enabled (Paul M and I confirmed noqueries was in the ntp.conf file.
- Though we couldn’t find any NTP bug reports for this issue, recommended they update to v5.7.0 (updating NTP from 4.2.8p9 to 4.2.8p10) and then rescan it.

### ShadowServer foundation/scanner

Per <https://ntpscan.shadowserver.org/>

Established in 2004, The Shadowserver Foundation gathers intelligence on the darker side of the internet. We are comprised of volunteer security professionals from around the world. Our [mission](#) is to understand and help put a stop to high stakes cybercrime in the information age.

The Shadowserver Foundation is currently undertaking a project to search for publicly accessible devices that have NTP running and answering Mode 6 queries. The goal of this project is to identify openly accessible NTP services and report them back to the network owners for remediation.

### Methodology

We are querying all computers with routable IPv4 addresses that are not firewalled from the internet on port 123/udp with an NTPv2 request for **READVAR** control message. We are capturing the response from the NTP service and parsing the result. We intend no harm, but if we are causing problems, please contact us at gro [tod] revreswodahs [ta] nacssnd

If you would like to test your own device to see if it supports Mode 6 queries, try the command: "**ntpq -c rv [IP]**". If the command is successful, you will see a string of information from the IP that you queried that usually starts off with something like this: 'associd=0 status=0615 leap\_none, sync\_ntp, 1 event, clock\_sync, version="ntpd 4.2.6p2@1.2194-o Sun Oct 17 13:35:13 UTC 2010 (1)", processor="x86\_64", system="Linux/3.2.0-0.bpo.4-amd64", leap=00'.

My testing with our SecureSyncs using the ntpq -c rv command (10.2.100.177 is running v5.5.1)

**A) With NTP Queries disabled on 10.2.100.177 (using CLI of 10.2.100.176)**

```
spadmin@Spectracom /usr/lib/gcc $ ntpq -c rv 10.2.100.177
10.2.100.177: timed out, nothing received
***Request timed out
```

**B) With NTP Queries enabled on 10.2.100.177 (using CLI of 10.2.100.176)**

```
spadmin@Spectracom /usr/lib/gcc $ ntpq -c rv 10.2.100.177
version="ntpd 4.2.8p9@1.3265-o Tue Nov 22 18:34:45 UTC 2016 (1)",
processor="i586", system="Linux/4.0.5-gentoo", leap=00, stratum=15,
precision=-18, rootdelay=0.000, rootdisp=0.000, refid=127.0.0.1,
offset=0.0000000 Thu, Feb 7 2036 6:28:16.000,
clock=dce56a0b.2c1f1e6d Fri, Jun 9 2017 18:40:11.172, peer=0, tc=3,
ntc=3, offset=0.000000, frequency=-20.039, sys_jitter=0.000000,
clk_jitter=0.004, clk_wander=0.000
```

Stuart (co-op) even went as far as using tcpdump to confirm what is being sent out with noquery, as compared to queries enabled.

This appears to be an issue in NTP itself, associated with at least one NTPQ command responding even with queries disabled (nessus is sending a command which gets through).

**(With queries disabled)**

Commands such as the peers (pe) command seems to be being blocked correctly by queries disabled. But commands such as version still respond with queries disabled.

for a description of each command, refer to:

[https://www.ibm.com/support/knowledgecenter/en/ssw\\_aix\\_61/com.ibm.aix.cmds4/ntpq.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_aix_61/com.ibm.aix.cmds4/ntpq.htm)

```
ntpq> help
ntpq commands:
:config drefid mreadlist readvar
addvars exit mreadvar reslist
apeers help mrl rl
associations host mrulist rmvars
authenticate hostnames mrv rv
authinfo ifstats ntpversion saveconfig
cl iostats opeers showvars
clearvars kerninfo passociations sysinfo
clocklist keyid passwd sysstats
clockvar keytype peers timeout
config-from-file lassociations poll timerstats
cooked lopeers pstats version
cv lpassociations quit writelist
debug lpeers raw writevar
delay monstats readlist
```

## NTP peers command (ntpq -p or ntpq -pn)

- Refer to: <http://doc.ntp.org/4.1.0/debug.htm>
- Lists all configured NTP inputs and reports statistics of each
- Type ntpq -pn at the command prompt (the “n” changes “names” to IP addresses to alleviate confusion)
- If already in “ntpq>”, just type **pe** <enter> to repeat the command (As shown in second screenshot below):

**Format of response:** [tally] remote refid st t when poll reach delay offset jitter (see examples)

“t” value

- u: unicast or manycast client
- b: broadcast or multicast client
- l: local (reference clock)
- s: symmetric (peer)
- A: manycast server
- B: broadcast server
- M: multicast server.

```
Linux 3.8.13-gentoo (tul) (2)
tul login: spadmin
Password:
Spectracon NetClock 9489 Version 5.1.2
spadmin@tul ~$ ntpq -p
=====
remote refid st t when poll reach delay offset jitter
=====
*PCI_TSYNC(0) .GPS. 0 1 1 16 377 0.000 0.014 0.002
oPPS(0) .PPS. 1 1 - 16 377 0.000 0.000 0.002
*10.2.100.93 .GPS. 1 u 7 8 377 0.301 -0.037 0.009
*spectracon.int. .PPS. 1 u 6 8 377 0.273 0.002 0.008
spadmin@tul ~$
```

```
ntpq> pe
=====
remote refid st t when poll reach delay offset jitter
=====
*PCI_TSYNC(0) .GPS. 0 1 16 16 377 0.000 0.014 0.002
oPPS(0) .PPS. 0 1 15 16 377 0.000 0.001 0.002
```



### “Tally Code”:

**Sync (“Tally Code”):** a symbol that indicates if the listed reference is available for selection as a reference. The following table indicates the symbols and their meanings.

| Tally code | Green = (Sync)<br>Red = (Not in Sync) (if the Reach is not 0)                                                                         | Truechimer (good) or<br>falsetickeer (bad)<br>(as determined by the<br>Clock Select Algorithm) |
|------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| *          | The Selected Time reference                                                                                                           | Truechimer                                                                                     |
| o          | The Selected PPS reference                                                                                                            | Truechimer                                                                                     |
| +          | A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected) | Truechimer                                                                                     |
| x          | “Falsetickeer” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).                            | falsetickeer                                                                                   |
| -          | “Outlyer” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).                                 | falsetickeer                                                                                   |
| (blank)    | Source discarded: Failed Sanity check                                                                                                 | falsetickeer                                                                                   |

## Fields of the ntpq -p / ntpq -pn response

- refer to: <https://www.eecis.udel.edu/~mills/ntp/html/ntpq.html>

```
peers
Display a list of peers in the form
[stat]:source refid st when poll reach delay offset jitter
Variable Description
[stat]: single-character code indicating current value of the stat field of the peer status word
source host name (or IP number) of peer
refid association ID or bias code
st stratum
t -1: unicast or multicast client; 0: broadcast or multicast client; 1: local (reference clock); a: symmetric (peer); s: manycast server; b: broadcast server; m: multicast server
when sec/min/hr since last received packet
poll poll interval (log2 s)
reach reach shift register (octal)
delay roundtrip delay
offset offset of server relative to this host
jitter jitter
```

- **refid** column shows the current source of synchronization (see details further below)
- **st** column reveals the stratum
- **t** the type (u = unicast, m = multicast, l = local, - = don't know),
- **poll** the poll interval in seconds.
- **when** column shows the time since the peer was last heard in seconds.
- **reach** column shows the status of the reachability register (in octal).

an 8-bit left-rotating register. Any 1 bit means that a "time packet" was received. The right most bit indicates the status of the last connection with the NTP server. It is Octal number. Use calculator in programmer interface to translate from OCT to BIN: For example, 377 translates to 11111111. Each 1 means a successful connection to the NTP server. If you just start a NTP service, and it connects successfully with its server, this number will change as follows (assuming connectivity is good):

```
00000001 = 001
00000011 = 003
00000111 = 007
00001111 = 017
00011111 = 037
00111111 = 077
01111111 = 177
11111111 = 377
```

### (Delay, offset and jitter in milliseconds).

- **delay** indicates the roundtrip time, in milliseconds, to receive a reply
- **offset** indicates the time difference, in milliseconds, between the client server and source

**Email Keith sent about Offset (24 Jul 17)** The NTP Offset is the time offset (reported in milliseconds) between this NTP device and the reference it's directly syncing with (as calculated by NTP). When an NTP client's time source is co-located at the same site and on the same subnet, this offset is usually very low (with ntpd, this value is typically 1 to 10 ms, while the Legacy VelaSync typically provides better NTP performance).

However, if there are several network hops between this NTP client and its NTP sever, the Offset value can become much higher, directly due to asymmetric path delays between the two NTP devices. As NTP can only measure the path delay in one direction, any time differences between this delay and the return path delay cannot be compensated for. So it becomes an automatic time Offset between it and its NTP Time source.

For instance, if the network delay between an NTP client and the Legacy VelaSync is 10 milliseconds in one direction, but due to the variance in return path, the delay in the other direction is only 5ms. NTP is going to account for the original 10ms delay. it can't account for the 5ms difference in the return path, so this results in a 5ms offset between the client and the server.

Other variables can also minimally influence the Offset value (such as hardware time stamping, versus software time stamping). But asymmetric path delays due to multiple network hops in between causing asymmetric delays is usually the biggest factor in how large the NTP offset value will be.

For example, I have seen cases where the Client and Server are located on the opposite sides of the US, and the offset value is in the tens of milliseconds (such as around 90ms or even higher) due to asymmetric path delay, as a direct result of changing network paths in one direction compared to the opposite direction. Minimizing the number of hops between the client and its time server helps to minimize the asymmetric delays that NTP can't account for, thereby decreasing the time Offset between the two devices.

- **jitter** indicates the difference (in milliseconds) between two samples



## NTP RefID / Reference ID (.gps, .pps, .init, .drop, .step, etc)

2. Refer to sites such as: <http://www.eecis.udel.edu/~mills/ntp/html/decode.html#kiss>

### A) .INIT

- should only remain “.init” until after about the initial NTP packet return from the SecureSync
- Indicates the NTP mode of the reference has not yet been identified (see additional info further below).
- “.init” is **494e4954** (in hex)
- Indicates NTP is trying to reach the reference for the first time, but can't initiate communications with this reference.
- Most likely causes:
  - The default gateway is not configured or not configured correctly, or
  - There is a network issue with port 123, or
  - NTP symmetric key is being enforced, but not correctly configured in all devices (preventing auth from being successful)

### To troubleshoot “.init” refID not changing shortly after NTP has started

1. is the “.init” SecureSync able to sync any other NTP clients
2. Does the “.init” SecureSync respond to pings (If no response, likely network issue or problem with the “.init” SecureSync)
3. perform a **traceroute -p 123 xxx.xxx.xxx** CLI call to the init SecureSync
4. verify it's a valid NTP server that is known to be up and running.
5. Check if **NTP Symmetric key authentication** is being enforced in either SecureSync

To determine if a SecureSync requires successful symmetric key authentication, on the left side of the **Management** -> NTP Setup page of the browser, click the **“Access Restrictions”** button. In the pop-up window, see if there is a **“1”** in the first row (for “IP4”), for the **“Auth Only”** column (as shown below):



| Type  | IP Version | IP      | IP Mask | Auth Only | Disable Query |                  |
|-------|------------|---------|---------|-----------|---------------|------------------|
| Allow | IPv4       | default |         | 1         |               | Change<br>Delete |
| Allow | IPv6       | default |         |           |               | Change<br>Delete |

**email Keith sent about “.init and symmetric authentication: (18 Dec 2018)** I was just talking with one of our Apps Engineers about NTP's refid value of “.init”. In addition to this being the initial refid for a peer/server when NTP first starts-up (until it starts getting NTP responses back from the particular peer/server), I wasn't sure if NTP would continue reporting “.init” if there was a larger time error than its expecting

He said he didn't believe so, especially if the Reach value for this same NTP sever is remaining “0” as well. And the testing I've been performing shows this doesn't appear to be the case- time error doesn't affect “.init” and doesn't stop the reach from incrementing. These two values in ntpq -p just need to see a time stamp returned.

But I just thought of another factor (besides a firewall in between blocking port 123) which I suspect could very well also affect both items— NTP symmetric key authentication, (one SecureSync requiring it, while its peer/server SecureSync/NTP either not configured to use it, or not correctly configured with an identical keystring/digest, or a key not marked as trusted. Symmetric key is a function of NTP often required for

switches to sync to an NTP server, especially Cisco switches.

After first verifying normal/expected NTP peering operation (Reach incrementing and "init" changing mere moments later) with no symmetric keying configured, I then ran a simple test to see if NTP symmetric key, if not correctly configured in both SecureSyncs, will prevent "init" from changing/Reach from incrementing for a peer.

I had "B" peered to "A" and told "A" to require symmetric key (even though "B" has no keys configured). This provided a case where successful authentication isn't possible. As I suspected, just like if there was a network issue between the two SecureSyncs – such as port 123 being closed, the Reach value stayed 0 and the refid stayed init for the peer which was not able to successfully authenticate.

Based on this observation that it definitely affects init and Reach, I now suspect the issue you are observing is that there is a symmetric key configuration mis-match between the "init" server and the other SecureSync(s).

If the server that you were running ntpq -p command on has been configured to require authentication (not the factory default state), and its peer(s) SecureSync is not configured with an identical keystring, this will prevent them from peering to each other, as exactly as you are seeing.

To determine if a SecureSync requires successful symmetric key authentication, on the left side of the **Management** -> NTP Setup page of the browser, click the **"Access Restrictions"** button. In the pop-up window, see if there is a "1" in the first row (for "IP4"), for the **"Auth Only"** column (as shown below)



| Type  | IP Version | IP      | IP Mask | Auth Only | Enable Query |                                                                    |
|-------|------------|---------|---------|-----------|--------------|--------------------------------------------------------------------|
| Allow | IPv4       | default |         | 1         |              | <input type="checkbox"/> Change<br><input type="checkbox"/> Delete |
| Allow | IPv6       | default |         |           |              | <input type="checkbox"/> Change<br><input type="checkbox"/> Delete |

If this field is blank, this SecureSync doesn't require successful authentication in order to exchange NTP packets with other NTP clients/other SecureSyncs. But if there is a "1" in the field (as shown above) symmetric key is being enforced and so it will only exchange NTP packets with other devices which are configured with an identical keystring.

Next, to see what trusted symmetric keys, if any, have been added to every SecureSync desired to be peered together (and every NTP client you wish to sync to the SecureSync), click the **"Symmetric Key"** button, also on the left side of the **Management** -> **NTP setup** page. The pop-up table will be empty if there are no keys configured. Or it will list a key ID, digest and a keystring, for each configured key



| Trusted                             | Key ID | Digest | Key String |                                                                    |
|-------------------------------------|--------|--------|------------|--------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | 1      | MD5    | 12345678   | <input type="checkbox"/> Change<br><input type="checkbox"/> Delete |

For authentication to be successful between an NTP server requiring authentication and another NTP device, the Key IDs don't have to match (they can, though it's not necessary), but:

the keystring on both NTP devices have to be IDENTICAL

the Trusted checkbox needs to be selected (which will place a "1" in the Trusted field for each key listed in the SecureSync)

if the Keys table for the SecureSync requiring auth has at least one key in it and its marked as Trusted, but the other NTP server has no keys listed, none of the keystrings are identical and/or a key with a matching string isn't marked as trusted, this is the problem. You will need to either create a new key having the trusted box selected and a matching keystring, or edit an existing incorrect key to make it a trusted/matching key.

To add a new Symmetric key, press the "+" sign in the upper-right corner of the "symmetric key table" (after pressing the Symmetric keys button on the left side of the NTP Setup page). The pop-up will look like the following screenshot. Select the Trusted box, enter an arbitrary Key ID Number, match the Digest Scheme selected in the other servers, and enter the identical key string. Then press Submit.

IP Symmetric Key

Trusted  Trusted

Symmetric Key ID

Digest Scheme MD5

Symmetric Key String

Apply

Note that most Cisco switches use MD5 for the Message Digest, but SecureSyncs also optionally support several other digests, also (such as SHA and SHA1 for examples)

---

## B) .DROP

The Reference identifier shows the word “**DROP**” in a Peer status. This appears to be due two units being peered, but when NTP starts up, only one of the two is in sync while the other is not in sync. If they both don't start at the same stratum, peering does not seem to work.

If the antenna or other reference is not connected, do not list each other as peers. Instead, list the one that is synced as a NTP server in the “Servers” table of the other unit that is not synced to a reference. Then restart NTP. Example below:

*MILFORD (Antenna attached)*

| NTP Reference Status: |              |        |         |                  |         |             |            |                     |       |            |             |             |
|-----------------------|--------------|--------|---------|------------------|---------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| Sync                  | Host         | Ref ID | Stratum | Mode             | Type    | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (mS) | Offset (mS) | Jitter (mS) |
| *                     | Spectracom   | GPS    | 0       | Client           | local   | none        | 65         | 64                  | 377   | 0.000      | 0.063       | 0.002       |
|                       | 172.20.75.10 | ?      | 16      | Symmetric Active | unicast | none        | 12         | 128                 | 0     | 0.000      | 0.000       | 4000.000    |

*Jefferson (No Antenna)*

| NTP Reference Status: |              |        |         |                  |         |             |            |                     |       |            |             |             |
|-----------------------|--------------|--------|---------|------------------|---------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| Sync                  | Host         | Ref ID | Stratum | Mode             | Type    | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (mS) | Offset (mS) | Jitter (mS) |
|                       | Spectracom   | LCL    | 0       | Client           | local   | none        | 0          | 16                  | 0     | 0.000      | 0.000       | 4000.000    |
|                       | 172.23.75.10 | DROP   | 16      | Symmetric Active | unicast | none        | 0          | 16                  | 0     | 0.000      | 0.000       | 4000.000    |

---

## C) .USER

- “.user” is “55534552” in hex
- System Time has been manually set using the user reference.

---

## D) .STEP

- A step time change in system time has occurred, but the association has not yet resynchronized.
- Time change of less than the panic threshold of 1000 seconds (16 min 40 sec) occurred.

---

## E) .DENY

- NTP access was denied by the NTP server

---

## F) .BCST

- NTP broadcast time server

---

## G) \*\*.PPS (atom clock driver/Enable Stratum 1 1 PPS checkbox)

- Refer to sites such as <http://www.eecis.udel.edu/~mills/ntp/html/drivers/driver22.html>
- “.PPS” is “50505300” in hex
- As long as the “**Enable Stratum 1PPS**” checkbox (newer browser) or “**Timing System 1PPS Reference**” field is “Enabled” (classic interface) in the NTP Servers tab, NTP can select the System PPS reference, if it wishes to (it's not guaranteed that it will). When Enabled, the Status -> NTP page of the browser will list System PPS as an NTP reference for NTP selected. But if it's an “X”, NTP won't be able to select it as a reference.
- If the “**Enable Stratum 1PPS**” checkbox (newer browser) or “Timing System 1PPS Reference” field is “Disabled” (classic interface) in the NTP Servers tab, the Status -> NTP page wont list system PPS as a possible reference for NTP input. So it can't be selected.
- It can take several minutes for NTP to select System PPS, if it desires to select it.

**Per Ron Dries** (7 July 2020) None of the servers in the ntp.conf file are marked as preferred. The PPS clock driver needs a serve marked as preferred to sync to it

**Note:** When NTP servers or peers have been configured, the “**Enable Stratum 1 PPS**” checkbox (newer browser) or “**Timing System 1PPS Reference**” field” (classic interface) should be disabled.

---

### Newer web browser (versions 5.1.2 and above)

Once NTP has synced to GPS inside the SecureSync (and assuming the “**Enable Stratum 1 PPS**” checkbox is Enabled in the **Management -> NTP Setup** page of the browser, **Stratum 1** tab, after pressing the “gear” icon to the right of “NTP Services” as shown below), we enable another NTP input reference that uses the 1PPS generated by the GPS signal. This “PPS” reference helps stabilize/optimize the NTP functionality, if NTP decides to select it as its input. This input is known as NTP’s PPS clock driver and can be selected by NTP shortly after NTP syncs to GPS. If NTP selects it as its reference, NTP changes the Ref ID to “.PPS” to indicate this PPS clock driver had been enabled.



**Per Ron Dries** (7 July 2020) None of the servers in the ntp.conf file are marked as preferred. The PPS clock driver needs a serve marked as preferred to sync to it

## NTPQ Associations (as)

- Refer to: <http://doc.ntp.org/4.1.0/debug.htm>
- Provides detailed info for each peer/server
- Requires “enable queries” (for NTPQ/NTPDC) to be Enabled (disabled by default) to obtain external to the SecureSync

### To enable NTPQ/NTPDC queries:

In the newer black browser: **Management** -> **NTP Setup** page and click **Access Restrictions** on the left side of the page. Press Change and enable Queries.

1. Need to first define the “host” as this particular time server.
  - Use the command of **host xxx.xxx.xxx.xxx** <enter> (where x is the IP address of the time server).
2. Type **as** <enter>

```

ntpq> host 10.2.100.176
current host set to 10.2.100.176
ntpq> as

ind assid status conf reach auth condition last_event cnt
=====
 1 28612 963a yes yes none sys.peer sys_peer 3
 2 28613 974a yes yes none pps.peer sys_peer 4
 3 28614 8011 yes no none reject mobilize 1
 4 28615 8011 yes no none reject mobilize 1
 5 28616 9424 yes yes none candidate reachable 2

```

**Condition column: Displays current NTP selection**  
**sys.peer:** System peer (current selected reference)  
**pps.peer:** PPS peer (current selected PPS reference)  
**candidate:** included by the combime algorithm (OK)  
**falsesticker:** currently discarded by the intersection algorithm  
**outlier:** currently discarded by the cluser algorithm (big offset)  
**reject:** currently discarded as not valid (not currently selectable)

**Last\_event column: Most recent event message received**  
**sys\_peer:** become system peer (if not already)  
**mobilize:** association mobilized (was previously rejected)  
**demobilize:** association demobilized (reject it now)  
**reachable:** server reachable  
**unreachable:** server unreachable  
**no reply:** no server found  
**Access denied:** Access denied by Peer's NTP configuration  
**Leap\_armed:** leap second to be applied

**Assid (AS command):** Correlates to the list of each peer shown in the **NTPQ -p** command. For example, **PCI\_Tsync<0>** equates to “28612” (first one in response)

The below Associations (AS) table is from: <http://doc.ntp.org/4.2.6/ntpq.html#clock>

| Variable   | Description                                                                                                                |
|------------|----------------------------------------------------------------------------------------------------------------------------|
| ind        | index on this list                                                                                                         |
| assid      | association ID <span style="border: 1px solid black; padding: 2px;">See table below</span>                                 |
| status     | <a href="#">peer status word</a>                                                                                           |
| conf       | yes: persistent, no: ephemeral                                                                                             |
| reach      | yes: reachable, no: unreachable                                                                                            |
| auth       | ok, yes, bad and none                                                                                                      |
| condition  | source (see <a href="#">peer status word</a> ) <span style="border: 1px solid black; padding: 2px;">See table below</span> |
| last_event | event report (see <a href="#">peer status word</a> )                                                                       |
| cnt        | event count (see <a href="#">peer status word</a> )                                                                        |

The below table is at: <http://doc.ntp.org/4.2.6/decode.html#sys>

**Peer Status Word**  
 The peer status word consists of four fields: Status (0-4, Select (5-7), Count (8-11) and Code (12-15). It is reported in the first line of the `peer` display produced by the `ntpq` program.

| Status | Select | Count | Code |
|--------|--------|-------|------|
| 0      | 5      | 8     | 12   |
| 1      | 6      | 9     | 13   |
| 2      | 7      | 10    | 14   |
| 3      |        | 11    | 15   |

The Status Field displays the peer status code bits in hexadecimal as follows:

| Code | Message | Description            |
|------|---------|------------------------|
| 08   | bcast   | broadcast association  |
| 10   | reach   | host reachable         |
| 20   | authamb | authentication enabled |
| 40   | auth    | authentication ok      |
| 80   | config  | persistent association |

The Select Field displays the current selection. The T Field displays the tally codes beginning the `ntpq peer` display. The values are coded as follows:

| Code | Message       | T | Description                                      |
|------|---------------|---|--------------------------------------------------|
| 0    | sel_reject    | T | discarded as not valid (TEST10-TEST13)           |
| 1    | sel_falsetick | x | discarded by intersection algorithm              |
| 2    | sel_excess    | . | discarded by table overflow (not used)           |
| 3    | sel_outlyer   | - | discarded by the cluster algorithm               |
| 4    | sel_candidate | + | included by the combine algorithm                |
| 5    | sel_backup    | # | backup (more than <code>maxclock</code> sources) |
| 6    | sel_sys_peer  | * | system peer                                      |
| 7    | sel_pps_peer  | o | PPS peer (when the prefer peer is valid)         |

The Count Field displays the number of events since the last time the code changed. Upon reaching 15, subsequent events with the same code are ignored. The Event Field displays the most recent event message coded as follows:

| Code | Message          | Description                          |
|------|------------------|--------------------------------------|
| 01   | mobillive        | association mobilized                |
| 02   | demobilive       | association demobilized              |
| 03   | unreachable      | server unreachable                   |
| 04   | reachable        | server reachable                     |
| 05   | restart          | association restart                  |
| 06   | no_reply         | no server found (ntpdate mode)       |
| 07   | rate_exceeded    | rate exceeded (kiss code RATE)       |
| 08   | access_denied    | access denied (kiss code DENY)       |
| 09   | leap_armed       | leap armed from server LI code       |
| 0a   | sys_peer         | become system peer                   |
| 0b   | clock_event      | see clock status word                |
| 0c   | bad_auth         | authentication failure               |
| 0d   | popcorn          | popcorn spike suppressor             |
| 0e   | interleave_mode  | entering interleave mode             |
| 0f   | interleave_error | interleave error (recovered)         |
| 10   | l2l...           | leapsecond values update from server |

**Per Ron Dries:**

Connect to the CLI interface (via an SSH session, using the same login credentials as the web browser). Then type the following command **ntpq -c associations**<enter>

This command will not show which key is being used, but it will show that authentication is being done between the two NTP devices!!

**Detailed synopsis (rv) for this server, or all servers on the network.**

- Refer to: <http://doc.ntp.org/3-5.93e/debug.html> and <http://doc.ntp.org/4.1.0/debug.htm>
- Provides detailed info for each peer/servers
- Requires “enable queries” (for NTPQ/NTPDC) to be Enabled to see all NTP servers on the network0 beyond just the one the command is being performed on. (disabled by default).

Next, use the **rv** command and the respective `assocID` identifier to display a detailed synopsis for the selected peer, such as “28612”).

From <http://doc.ntp.org/4.2.6/ntpq.html>

**RV:** Display the specified variables. If `assocID` is zero, the variables are from the [system variables](#) name space, otherwise they are from the [peer variables](#) name space. The `assocID` is required, as the same name can occur in both spaces. If no `name` is included, all operative variables in the name space are displayed. In this case only, if the `assocID` is omitted, it is assumed zero. Multiple names are specified with comma separators and without whitespace. Note that time values are represented in milliseconds and frequency values in parts-per-million (PPM). Some NTP timestamps are represented in the format

YYYYMMDDTTTT, where YYYY is the year, MM the month of year, DD the day of month and TTTT the time of day.

- There is one **system status word** and a **peer status word** for each association.
- **System status word** is the first line of the rv response

| Leap | Source | Count | Code |
|------|--------|-------|------|
|------|--------|-------|------|

- **Peer status word** is the first line of the rv response

| Status | Select | Count | Code |
|--------|--------|-------|------|
|--------|--------|-------|------|

- There is a **clock status word** for each association that supports a **reference clock** (our tsync driver)

1. **Type `rv yyyy`** <enter> (where yyyy is a particular **assid** number from the **as** response above (such as 28612 for example):

```
=====
 1 28612 963a yes yes none sys.peer sys_peer 3
 2 28613 974a yes yes none pps.peer sys_peer 4
 3 28614 8011 yes no none reject mobilize 1
 4 28615 8011 yes no none reject mobilize 1
 5 28616 9424 yes yes none candidate reachable 2
ntpq> rv 28616
associd=28616 status=9424 conf, reach, sel_candidate, 2 events, reachable,
srcadr=10.2.100.177, srcport=123, dstadr=10.2.100.176, dstport=123,
 leap=00, stratum=1, precision=-19, rootdelay=0.000, rootdisp=0.244,
 refid=PPS, reftime=d867f7c1.b10e0ac9 Mon, Jan 19 2015 21:38:09.691,
 rec=d867f7c3.a2a9d6f5 Mon, Jan 19 2015 21:38:11.635, reach=377,
 unreach=0, hmode=1, pmode=2, hpoll=3, ppoll=3, headway=4, flash=00 ok,
 keyid=0, offset=0.019, delay=0.211, dispersion=0.715, jitter=0.254,
 xleave=0.073,
 filtdelay= 0.89 0.89 0.87 0.87 0.22 0.22 0.21 0.21,
 filtoffset= -0.32 -0.31 -0.32 -0.32 0.02 0.02 0.02 0.02,
 filtdisp= 0.00 0.12 0.24 0.36 0.48 0.60 0.72 0.84
ntpq>
```

("AS" command response)

(see "System Variables" table further below)

**Note:** "filtdelay", "filtoffset" and "filtdisp" (shown at the bottom of the "rv 28616" response screenshot above)



2. Can also type just `rv` without an assid number (as shown below):

```

ntpq> rv
associd=0 status=0115 leap none, sync_pps, 1 event, clock_sync,
version="ntpd 4.2.6p5@1.2349-o Sat Jun 29 08:10:49 UTC 2013 (1)",
processor="i586", system="Linux/3.8.13-gentoo", leap=00, stratum=1,
precision=-19, rootdelay=0.000, rootdisp=0.305, refid=PPS,
reftime=d867f5d8.a2669d64 Mon, Jan 19 2015 21:30:00.634,
clock=d867f5dd.72e3b594 Mon, Jan 19 2015 21:30:05.448, peer=28613, tc=4,
mintc=3, offset=0.010, frequency=-18.357, sys_jitter=0.002,
clk_jitter=0.002, clk_wander=0.003
ntpq>

```

(see "System Variables" table below)

**Note:** "filtdelay", "filtoffset" and "filtdisp" (shown at the bottom of the "rv 28616" response screenshot further above) are not reported when "rv" is performed with adding an association number (as show in the screenshot directly above).

Below is from: <http://doc.ntp.org/4.2.6/ntpq.html#clock>

#### System Variables

The following system variables appear in the `rv` billboard. Not all variables are displayed in some configurations.

| Variable   | Description                                           |
|------------|-------------------------------------------------------|
| status     | <a href="#">system status word</a>                    |
| version    | NTP software version and build time                   |
| processor  | hardware platform and version                         |
| system     | operating system and version                          |
| leap       | leap warning indicator (0-3)                          |
| stratum    | stratum (1-15)                                        |
| precision  | precision ( $\log_2$ s)                               |
| rootdelay  | total roundtrip delay to the primary reference clock  |
| rootdisp   | total dispersion to the primary reference clock       |
| peer       | system peer association ID                            |
| tc         | time constant and poll exponent ( $\log_2$ s) (3-17)  |
| mintc      | minimum time constant ( $\log_2$ s) (3-10)            |
| clock      | date and time of day                                  |
| refid      | reference ID or <a href="#">kiss code</a>             |
| reftime    | reference time                                        |
| offset     | combined time offset                                  |
| sys_jitter | combined system jitter                                |
| frequency  | clock frequency offset (PPM)                          |
| clk_wander | clock frequency wander (PPM)                          |
| clk_jitter | clock jitter                                          |
| tai        | TAI-UTC offset (s)                                    |
| leapsec    | NTP seconds when the next leap second is/was inserted |
| expire     | NTP seconds when the NIST leapseconds file expires    |

The jitter and wander statistics are exponentially-weighted RMS averages. The system jitter is defined in the NTPv4 specification; the clock jitter statistic

Peer variables table (<http://doc.ntp.org/4.2.6/ntpq.html>)

**Peer Variables**

The following system variables appear in the `≡` billboard for each association. Not all variables are displayed in some configurations.

| Variable                                    | Description                                                                 |
|---------------------------------------------|-----------------------------------------------------------------------------|
| <code>associd</code>                        | association ID                                                              |
| <code>status</code>                         | <a href="#">peer status word</a>                                            |
| <code>srcadr</code><br><code>srcport</code> | source (remote) IP address and port                                         |
| <code>dstadr</code><br><code>dstport</code> | destination (local) IP address and port                                     |
| <code>leap</code>                           | leap indicator (0-3)                                                        |
| <code>stratum</code>                        | stratum (0-15)                                                              |
| <code>precision</code>                      | precision ( $\log_2 s$ )                                                    |
| <code>rootdelay</code>                      | total roundtrip delay to the primary reference clock                        |
| <code>rootdisp</code>                       | total root dispersion to the primary reference clock                        |
| <code>refid</code>                          | reference ID or <a href="#">kiss code</a>                                   |
| <code>reftime</code>                        | reference time                                                              |
| <code>reach</code>                          | reach register (octal)                                                      |
| <code>unreach</code>                        | unreach counter                                                             |
| <code>hmode</code>                          | host mode (1-6)                                                             |
| <code>pmode</code>                          | peer mode (1-5)                                                             |
| <code>hpoll</code>                          | host poll exponent ( $\log_2 s$ ) (3-17)                                    |
| <code>ppoll</code>                          | peer poll exponent ( $\log_2 s$ ) (3-17)                                    |
| <code>headway</code>                        | headway (see <a href="#">Rate Management and the Kiss-o'-Death Packet</a> ) |
| <code>flash</code>                          | <a href="#">flash status word</a>                                           |
| <code>offset</code>                         | filter offset                                                               |
| <code>delay</code>                          | filter delay                                                                |
| <code>dispersion</code>                     | filter dispersion                                                           |
| <code>jitter</code>                         | filter jitter                                                               |
| <code>bias</code>                           | unicast/broadcast bias                                                      |
| <code>xleave</code>                         | interleave delay (see <a href="#">NTP Interleaved Modes</a> )               |

## NTP Status/Statistics graphs (NTP Throughput graphs, NTP Performance graphs, Time Offset graph)

- Refer to online SecureSync user guide at:
- NTP Status Graphs are in the **Management** -> **NTP Setup** page of the the newer browser.

Excerpt below from the online SecureSync user guide

[http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_SetupScreen.htm?Highlight=ntp%20graphs](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_SetupScreen.htm?Highlight=ntp%20graphs)

### The NTP Throughput panel

shows two graphs depicting the rate of NTP traffic from Clients and Server/Peers.

- The INFO icon opens a window showing the maximum per second traffic rate from each.
- The graphs may be saved and downloaded (> ARROW icon), or deleted (> TRASH CAN icon).
- Note that this data is currently only displayed for NTP, and not for TimeKeeper NTP.

### NTP Performance Graphs

**NTP data for the NTP performance graphs (Time Offset, Freq Offset and Jitter) (v5.1.2 and higher) located on the left side of the NTP Setup page**

- The graphs are generated using the NTP data (clockstats, peerstats and sysstats) stored in the NTPStats folder (/home/spectracom/logs/ntpstats)
- The graph data is included in the log bundle.

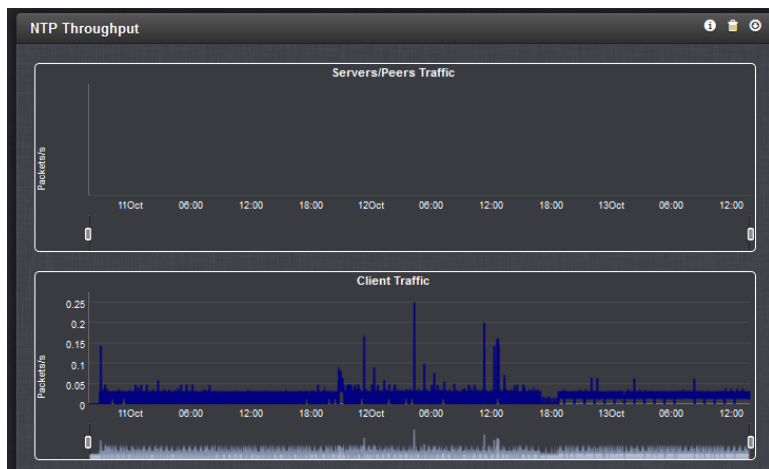
```
factory@spectracom /home/spectracom/log # cd ntpstats
factory@spectracom /home/spectracom/log/ntpstats $ ls
clockstats loopstats peerstats.20151015 sysstats.20151015
clockstats.20151015 loopstats.20151015 peerstats.20151016 sysstats.20151016
clockstats.20151016 loopstats.20151016 peerstats.20151017 sysstats.20151017
clockstats.20151017 loopstats.20151017 peerstats.20151018 sysstats.20151018
clockstats.20151018 loopstats.20151018 peerstats.20151019 sysstats.20151019
clockstats.20151019 loopstats.20151019 sysstats
put.plot peerstats sysstats.20151014
```

- For more information on the breakdown of this NTP data, refer to the following page of the ntp website: <https://www.eecis.udel.edu/~mills/ntp/html/monopt.html>

**Recommendation to be able to better review these files:** Rename the files with the extension of **“.CSV”** . The file will still open with Excel, but the comma delimited values will be in separate columns, instead of all values being in the same column when just opening as a standard excel file.

## NTP throughput graphs/throughput logs

Versions 5.3.1 and higher (version 5.3.1 added NTP throughput graphs)



- In addition to the existing NTP Status graphs (discussed below), software version 5.3.1 added NTP throughput graphs/NTP Traffic graphs (The “Servers/Peers Traffic” and “Client traffic” graphs) to the Management -> NTP Setup page of the browser.
- Reports packets being exchanged each second.

### Where:

- **Clients:** NTP requests from NTP clients on the network
- **Servers/Peers:** NTP requests from Servers or Peers configured to get time from this SecureSync

### A) To convert pkt/s (values in the graphs/logs) to the actual number of packets in the hour

**Multiply** the number of pkt/s (value in the graphs/logs) times **60** and then round-up to nearest whole number

Examples:

- 0.017 pkt/s = 1** packet in one hour
- 0.083 pkt/s = 5** packets in one hour
- 0.167 pkt/s = 10** packets in one hour
- 1.667 pkt/s = 100** packets in one hour
- 166.667 pkt/s = 10,000** packets in one hour
- 3000 pkt/s = 180,000** packets in one hour

### B) To convert actual number of packets per hour to pkt/s (values in the graphs/logs)

**Divide** the number of ntp packets in the hour by **60** (there are 60 minutes in the report period)

Examples:

- 1 packet in one hour = **0.017 pkt/s**
- 5 packets in one hour = **0.083 pkt/s**
- 10 packets in one hour = **0.167 pkt/s**
- 100 packets in one hour = **1.667 pkt/s**
- 10,000 packets in one hour = **166.667 pkt/s**
- 180,000 packets in one hour = **3000 pkt/s**

---

Downloading the NTP throughput graph data

## Download graph data as a .csv file

NTP Graph Data can be downloaded (using down arrow icon) or deleted (using the garbage can icon). The file is named “LogNTPStat.csv”.

| id | sys_timestamp    | ntp_client | ntp_server |
|----|------------------|------------|------------|
| 1  | 10/10/2016 19:47 | 0          | 0          |
| 2  | 10/10/2016 19:48 | 0          | 0          |

## Download graph data using the CLI interface (instead of downloading a .csv file via the browser, as with heavy loading/earlier versions of software like v5.3.1 “hanging” when trying to download the data)

The NTP throughput data is stored in the mysql database, which is contained in the log bundle. Via CLI - The log bundle file can be generated (**savelog securesync.log** command) and the exported from the **home/spectracom/xfer/log** directory using FTP/SCP.

**Email Keith sent (12 Oct 16)** The data for the NTP throughput graphs displayed on the bottom of the **Management** -> **NTP Setup** page of the browser can be exported out of the time server as either a .csv file, or inside a log bundle. The log bundle is a single file containing all of the unit’s log entries and other data. This log bundle file can be exported using either the browser or the CLI interface (telnet/ssh to generate the file and FTP/SCP to download the file to a computer).

This log bundle file can be generated and automatically downloaded to a PC using the “**Save and Download All Logs**” button on the left-side of the **Management** -> **Log Configuration** page of the browser. To download the file using the CLI interface (instead of using the web browser) first establish a telnet/ssh session and then type the following command: **savelog securesync.log** (where securesync.log is an arbitrary name for this file) as shown below:

```
spadmin@Spectracom /home/spectracom $ savelog securesync.log
/home/spectracom/xfer/log/securesync.log
Creating Log Archive at /home/spectracom/xfer/log/securesync.log
Deleting old Log Archive file...
tar: Removing leading '/' from member names
tar: Removing leading '/' from hard link targets
spadmin@Spectracom /home/spectracom $
```

This bundle file is generated and saved in the **home/spectracom/xfer/log** directory (as shown below). This file can then be transferred out of the unit via an FTP or SCP connection to this directory.

```
tar: Removing leading '/' from hard link targets
spadmin@Spectracom /home/spectracom $ cd xfer/log
spadmin@Spectracom /home/spectracom/xfer/log $ ls
securesync.log
spadmin@Spectracom /home/spectracom/xfer/log $
```

This log bundle file is tarred twice to decrease its size as much as possible for being able to email it to us for review. Once the file has been downloaded via either the web browser or the CLI interface, first untar this file and then untar again the file that is generated from the first untarring. The file will probably be around 30 MB or so once its been fully untarred.

With versions 5.3.1 and higher, there will be three separate folders in the untarred file. They are the **home**, **srv** and **var** files. Open the srv file and click through each of the folders that appear (**www2**, **app** and then **webroot**). This will lead you to the lafayette file. Rename this file as **lafayette.db**.

This **database** file can be opened using the freeware MySQL viewer program called “DB Browser for SQLite” (<http://sqlitebrowser.org>). After opening the DB browser program, click on **File** -> **Open Database** and navigate to the **lafayette.db** file. With the database now open in the DB Browser program, select the “**Browse Data**” tab at the top of the page. In the “**Table**” drop-down (just below the four tabs), select “**log\_ntp\_stats**”. The data for the NTP throughput graphs will now be displayed (and can be copy/pasted out as desired).

|   | id    | sys_timestamp   | ntp_client      | ntp_server |
|---|-------|-----------------|-----------------|------------|
| 1 | 60227 | 2016-08-23 1... | 0.3064516129... | 0.0        |
| 2 | 60226 | 2016-08-23 1... | 0.2950819672... | 0.0        |
| 3 | 60225 | 2016-08-23 1... | 0.2741935483... | 0.0        |
| 4 | 60224 | 2016-08-23 1... | 0.3114754098... | 0.0        |
| 5 | 60223 | 2016-08-23 1... | 0.2741935483... | 0.0        |
| 6 | 60222 | 2016-08-23 1... | 0.3223806451... | 0.0        |
| 7 | 60221 | 2016-08-23 1... | 0.4516120032... | 0.0        |
| 8 | 60220 | 2016-08-23 1... | 0.5396825396... | 0.0        |
| 9 | 60219 | 2016-08-23 1... | 0.4666666666... | 0.0        |

**FYI-** All the units logs that are displayed in the **Tools** drop-down of the browser, and a couple of other logs stored in the background, are located in the **home/spectracom/log** directory of the downloaded log bundle.

### Software issue with NTP Traffic Graphs in at least software versions 5.4.0, 5.4.1 and 5.4.5

**Note:** this issue was fixed in the version 5.5.1 update process (version 5.5.0)

- Paul Myers found an issue starting with version 5.4.0 (in at least versions 5.4.0, 5.4.1 and 5.4.5) where the log data in the mysql database may become too large to remove past data.
- SR 6349 in SAP (Sept 2016) is a report of the data being a couple of days behind current date. I suspect this is a symptom of this condition.
- Recommendation is to get a log bundle to review what data is in the database.

### A) Software issue with NTP Traffic Graphs in at least software version 5.3.1

- Refer to Mantis case 3189 / Salesforce case 20174
- On 10 Dec, 2015, Ron Dries found there is unintended averaging of the graph data being displayed.
- I believe this issue was addressed with a software change after v5.3.1

### NTP throughput also provided hourly in ntp logs

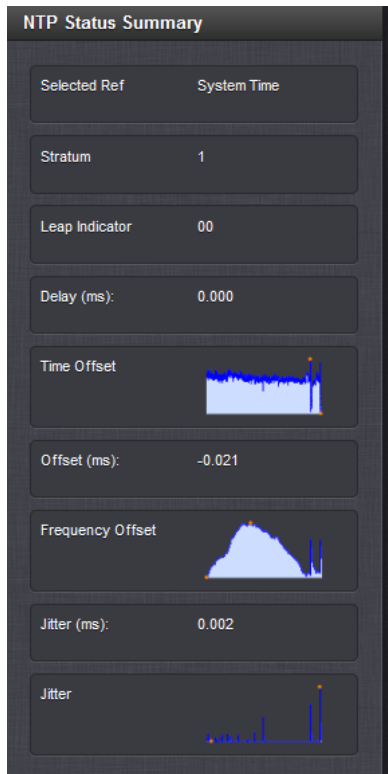
- Refer to (in this document):

### Versions 5.1.2 and higher

**Management** -> **NTP Setup** page of the browser (there is a separate tab for each graph) the graph is in the lower-left corner.

Note that it takes about 6 seconds for the information to be displayed once the page has been opened (delay is due to the time it takes for NTPQ to obtain the info from NTP)

Clicking on the Time Offset, Frequency Offset or Jitter graphs opens an expanded view of that graph.



## Versions 5.0.2 and below

**Status** -> **NTP** page of the browser (there is a separate tab for each graph)

| NTP INPUT STATUS |                    |         |    |            |             |            |             |            |             |
|------------------|--------------------|---------|----|------------|-------------|------------|-------------|------------|-------------|
| Name             | Selected Reference | Stratum | LI | Delay (ms) | Offset (ms) | 2000 Delay | 2000 Offset | 2000 Delay | 2000 Offset |
| 00               | System Time        | 1       | 01 | 0.000      | -0.021      | 0.000      | 0.000       | 0.000      | 0.000       |

| NTP Selected Reference Status |        |         |    |            |             |            |             |            |             |
|-------------------------------|--------|---------|----|------------|-------------|------------|-------------|------------|-------------|
| Name                          | Ref    | Stratum | LI | Delay (ms) | Offset (ms) | 2000 Delay | 2000 Offset | 2000 Delay | 2000 Offset |
| ✓                             | System | 1       | 01 | 0.000      | -0.021      | 0.000      | 0.000       | 0.000      | 0.000       |

| NTP Reference Status |        |         |    |            |             |            |             |            |             |
|----------------------|--------|---------|----|------------|-------------|------------|-------------|------------|-------------|
| Name                 | Ref    | Stratum | LI | Delay (ms) | Offset (ms) | 2000 Delay | 2000 Offset | 2000 Delay | 2000 Offset |
| ✓                    | System | 1       | 01 | 0.000      | -0.021      | 0.000      | 0.000       | 0.000      | 0.000       |

The graphs displayed in the NTP section have dynamic vertical scales. The bottom scale is the number of seconds since UTC midnight. The graph shows about 22 hours across.

### 1. Time Offset Graph

- Reports the time offset (in scientific notation) between NTP and its selected reference.

The vertical scales vary depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).

The scientific breakdown is as follows:

**1e-09 = 1 ns** or 0000.000000001

1e-08= 10 ns

1e-07= 100ns

**1e-06= 1 microsecond** or 0000.000001000

1e-05= 10 microseconds 0000.000010000

1e-04= 100 microseconds or 0000.000100000

**1e-03= 1 milliseconds** or 0000.001000000

1e-02= 10 milliseconds or 0000.010000000

1e-01= 100 milliseconds or 0000.100000000  
**1e+00=1 second** or 0001.000000000  
**1e+01= 10 Seconds** or 0010.000000000  
**1e+02= 100 Seconds** or 0100.000000000  
**1e+03= 1000 Seconds** 1000.000000000

**Note:** If the first digit isn't a "1", multiply the first digit by the "time" value in the table above

Examples

**2e-05**= 20 microseconds or 0000.000020000 ("2" times "10 microseconds" is 20 microseconds)  
**5e-06**= 5 microseconds or 0000.000050000 ("5" times "1 microseconds" is 5 microseconds)

---

## 2. RMS Jitter Graph

- Reports the variance in time offset (in seconds), from one calculation to the next
- Official definition: The value reported by NTP is the exponential average of the square root of the sum of the squares of past offset differences

When repeatedly reading the time, the difference may vary almost randomly. The difference of these differences (second derivation) is called jitter.

**Examples:**

0.000002 seconds = 2 microseconds  
0.0000019 seconds = 1.9 microseconds  
0.0000022 seconds = 2.2 microseconds

---

## 3. Frequency Offset Graph

- Reports how much time drift our kernel is experiencing, based on the frequency disciplining of NTP.
- This is the amount of time error our kernel time would have drifted, if NTP was not synced by a reference.
- Our typical frequency offset appears to be around 13 PPM (about one second per day).

From <http://www.ntp.org/ntpfaq/NTP-s-sw-clocks-quality.htm#AEN1230>

Unfortunately all the common clock hardware is not very accurate. This is simply because the frequency that makes time increase is never exactly right. Even an error of only 0.001% would make a clock be off by almost one second per day. This is also a reason why discussing clock problems uses very fine measures: One PPM (Part Per Million) is 0.0001% (1E-6).

Real clocks have a frequency error of several PPM quite frequently. Some of the best clocks available still have errors of about 1E-8 PPM (For one of the clocks that is behind the German DCF77 the stability is told to be 1.5 s/day (1.7E-8 PPM). See <http://www.ptb.de/english/org/4/43/432/real.htm> or [http://www.ptb.de/en/org/4/44/441/real\\_e.htm](http://www.ptb.de/en/org/4/44/441/real_e.htm)).

\*\*As most people have some trouble with that abstract PPM (parts per million, 0.0001%), I'll simply state that 12 PPM correspond to one second per day roughly. So 500 PPM means the clock is off by about 43 seconds per day.

**Examples**

- 12PPM = about one second per day of time drift.
- 69 PPM= about six seconds per day of time drift.
- 500 PPM= about 43 seconds per day of time drift.



---

## Identifying if NTP has selected the System PPS (atom clock driver)

- Using the ntpq -p command and the newer browser in versions 5.1.2 and above

### “NTP Servers” list on the NTP Setup page

#### System PPS (Atom clock driver) not yet selected by NTP (Ref ID not yet .pps)

- “System Time” will be in green and “(Sync)”
- “System 1 PPS” will still be in orange and reporting “(Initializing)”

| NTP Servers                                         |        |             |      |      |            |
|-----------------------------------------------------|--------|-------------|------|------|------------|
| IP/HOST                                             | REF ID | AUTH STATUS | LAST | POLL | DELAY (MS) |
| <input checked="" type="radio"/> SYSTEM TIME (SYNC) | .USER. | none        | 13   | 16   | 0.000      |
| <input type="radio"/> SYSTEM 1PPS (INITIALIZING)    | .PPS.  | none        | -    | 16   | 0.000      |

NTPQ -p command will have a “space” in front of “PPS (0)”

```
*PCI_TSYNC (0) .USER. 0 1 2 16 377 0.000 -0.100 0.033
 PPS (0) .PPS. 0 1 - 16 0 0.000 0.000 0.000
```

#### System PPS (Atom clock driver) selected by NTP (Ref ID is being as .pps)

- “System Time (Sync)” will be in green
- “System 1 PPS (Sync)” will be in green

| NTP Servers                                         |        |             |      |      |            |
|-----------------------------------------------------|--------|-------------|------|------|------------|
| IP/HOST                                             | REF ID | AUTH STATUS | LAST | POLL | DELAY (MS) |
| <input checked="" type="radio"/> SYSTEM TIME (SYNC) | .USER. | none        | 12   | 16   | 0.000      |
| <input checked="" type="radio"/> SYSTEM 1PPS (SYNC) | .PPS.  | none        | 11   | 16   | 0.000      |

NTPQ -p command will have a “circle” in front of “PPS (0)”

```
*PCI_TSYNC (0) .GPS. 0 1 11 16 377 0.000 0.010 0.002
 oPPS (0) .PPS. 0 1 10 16 377 0.000 -0.003 0.002
```

### Ntp.log entries for selecting/de-selecting the System PPS

- Software versions 5.0.0 and above (NTPv4.2.6): these changes aren’t logged.
- Software versions 4.8.9 and below (NTPv4.2.0): these changes are logged.

---

### Classic interface web browser

Once NTP has synced to GPS inside the SecureSync (and assuming the “Timing System 1PPS Reference” field is Enabled in the **Network** -> **NTP Setup** page of the browser, **NTP Servers** tab, as shown below), we enable another NTP input reference that uses the 1PPS generated by the GPS signal. This “PPS” reference helps stabilize/optimize the NTP functionality, if NTP decides to select it as its input. This input is known as NTP’s PPS clock driver and can be selected by NTP shortly after NTP syncs to GPS. If NTP selects it as its reference, NTP changes the Ref ID from “.GPS” to “.PPS” to indicate this PPS clock driver had been enabled.

## NTP SETUP

General Settings
NTP Peers
NTP Servers
Symmetrical Keys
Autokey
NTP Broadcasting
NTP Access

Timing System Reference
Enabled 
Preferred

Typically references like GPS or IRIG provide better accuracy than NTP.  
Check this box to use those references as the preferred timing input to NTP.  
Uncheck this box if NTP servers or peers are the only input references available.

Timing System 1PPS Reference
Enabled

If you are configuring NTP servers or peers as either the preferred reference or as a backup to the timing system, do not enable the timing system 1PPS reference.

If you look at the **Status -> NTP** page of the SecureSync's browser when the **Timing System 1PPS Reference** is enabled, you will see the following, with the NTP Reference Status table showing both .GPS and .PPS. Note that when the SecureSync is able to get time from other NTP servers (NTP Peer or NTP Server modes), we recommend the **"Timing System 1PPS Reference"** be set to disabled, in which case the PPS reference is not listed as a reference and not sent to NTP. In this case, it will always remain ".gps" instead of ".pps".

### NTP INPUT STATUS

Status
Time Offset
RMS Jitter
Frequency Offset

| Sync | Selected Reference | Stratum | LI | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|--------------------|---------|----|------------|-------------|-------------|
| Yes  | System Time        | 1       | 00 | 0.000      | -0.001      | 0.002       |

#### NTP Selected Reference Status

| Sync | Host        | Ref ID | Stratum | LI | Mode   | Type  | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|-------------|--------|---------|----|--------|-------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| --   | System Time | .GPS.  | 0       | 00 | Client | local | none        | 8          | 16                  | 377   | 0.000      | -0.001      | 0.002       |

#### NTP Reference Status

| Sync | Host         | Ref ID | Stratum | LI | Mode   | Type   | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|--------------|--------|---------|----|--------|--------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| --   | System Time  | .GPS.  | 0       | 00 | Client | local  | none        | 8          | 16                  | 377   | 0.000      | -0.001      | 0.002       |
| 'x'  | System PPS   | .PPS.  | 0       | 00 | Client | local  | none        | 6          | 16                  | 377   | 0.000      | -0.014      | 0.002       |
| ..   | 10.10.128.15 |        | 16      | 00 | Client | server | none        | 6          | 16                  | 0     | 0.126      | 18.186      | 0.000       |

## PKI (Public Key Infrastructure/Public Key cryptography) for NTP security

Refer to sites such as <http://www.ntp.org/ntpfaq/NTP-s-algo-crypt.htm> and the "NTP Security Model" Powerpoint at: <https://www.eecis.udel.edu/~mills/database/brief/autokey/autokey.ppt>

### NTP Security Model

- NTP operates in a mixed, multi-level security environment including symmetric key cryptography, public key cryptography and unsecured.
- NTP timestamps and related data are considered public values and never encrypted.
- Time synchronization is maintained on a master-slave basis where synchronization flows from trusted servers to dependent clients possibly via intermediate servers operating at successively higher stratum levels.
- A client is authentic if it can reliably verify the credentials of at least one server and that server messages

have not been modified in transit.

- A client is proventic if by induction each server on at least one path to a trusted server is authentic.

## \*\*NTP Symmetric Key Authentication (MD5/SHA1)/ntp.keys file

- Refer to: <http://doc.ntp.org/4.2.4/authopt.html>
- Symmetric key authentication can't be used in conjunction with NTP Autokey.

Refer to the “**NTP Restriction and MD5 Authentication**” Tech Note (which can be sent to customers):

<..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Restriction and Authentication-MD5 and SHA>

**NTP Access Restrictions:** Require/enforce NTP authentication for all NTP clients, versus allowing both Authenticated and Unauthenticated clients to receive timestamps

(excerpt below from the NTP Restrictions tech note)

To enforce NTP auth (the SecureSync will only respond to NTP clients that are using authentication, and the hash was properly authenticated with the SecureSync), is as follows:

### To reconfigure the SecureSync to only respond to properly authenticated time requests

- 1) Navigate to the **Management -> NTP Setup** page of the web browser.
- 2) Click on the “**Access Restrictions**” button (on the left side of the page).
- 3) In the pop-up window, click on the “**Change**” button at the end of the “IPv4 row” (or the “IPv6 row as applicable to the network”).



Figure 4: Location of the “Change” button

- 4) Select the checkbox for “**Require Authentication**”



Figure 5: “Require authentication” checkbox

Notes:

- A) When enabled, the “**Require Authentication**” checkbox forces all NTP clients to successfully authenticate with the time server, in order for the time server to respond with NTP time stamps. It’s typically recommended to leave this checkbox not selected
  - B) When enabled, the “**Allow NTP queries**” checkbox allows other nodes on the network to be able to perform NTPD and/or NTPDC (both are associated with NTP) queries on this time server. It’s typically recommended to leave this checkbox not selected.
- 5) Hit the Submit button.
  - 6) The NTP Service will now be automatically restarted.

**Note:** After restarting NTP, it will take a couple minutes for NTP to resynchronize and be a useable reference to the network

### **Not able to edit, create or delete symmetric keys while in Expert Mode**

- Refer to Mantis case 3041
- Expert mode disables browser NTP functions, so in at least versions 5.2.0 and below, users can’t get to the symmetric keys button and associated functions while expert mode is enabled.
- Work-around is to at least temporarily disable Expert mode, create new or edit existing symmetric keys and then re-enable Expert mode. Note that disabling Expert mode causes settings to be lost.

### **Number of available NTP keys which can be generated**

**Key ID:** The key ID must be a number between **1** and **65532**.

### **Acceptable characters (for ntp keys)**

- Max 20-character printable ASCII string or a 40-character hex string

**FYI:** the Symmetric key should be able to be any of the following printable characters (21 through 7F, Hex) with the exception of a space and a “#” sign (these two characters are not allowed). They key length can be up to **20 characters** long.

| Dec | Hx | Oct | Html  | Chr   | Dec | Hx | Oct | Html  | Chr | Dec | Hx | Oct | Html   | Chr |
|-----|----|-----|-------|-------|-----|----|-----|-------|-----|-----|----|-----|--------|-----|
| 32  | 20 | 040 | &#32; | Space | 64  | 40 | 100 | &#64; | @   | 96  | 60 | 140 | &#96;  | `   |
| 33  | 21 | 041 | &#33; | !     | 65  | 41 | 101 | &#65; | A   | 97  | 61 | 141 | &#97;  | a   |
| 34  | 22 | 042 | &#34; | "     | 66  | 42 | 102 | &#66; | B   | 98  | 62 | 142 | &#98;  | b   |
| 35  | 23 | 043 | &#35; | #     | 67  | 43 | 103 | &#67; | C   | 99  | 63 | 143 | &#99;  | c   |
| 36  | 24 | 044 | &#36; | \$    | 68  | 44 | 104 | &#68; | D   | 100 | 64 | 144 | &#100; | d   |
| 37  | 25 | 045 | &#37; | %     | 69  | 45 | 105 | &#69; | E   | 101 | 65 | 145 | &#101; | e   |
| 38  | 26 | 046 | &#38; | &     | 70  | 46 | 106 | &#70; | F   | 102 | 66 | 146 | &#102; | f   |
| 39  | 27 | 047 | &#39; | '     | 71  | 47 | 107 | &#71; | G   | 103 | 67 | 147 | &#103; | g   |
| 40  | 28 | 050 | &#40; | (     | 72  | 48 | 110 | &#72; | H   | 104 | 68 | 150 | &#104; | h   |
| 41  | 29 | 051 | &#41; | )     | 73  | 49 | 111 | &#73; | I   | 105 | 69 | 151 | &#105; | i   |
| 42  | 2A | 052 | &#42; | *     | 74  | 4A | 112 | &#74; | J   | 106 | 6A | 152 | &#106; | j   |
| 43  | 2B | 053 | &#43; | +     | 75  | 4B | 113 | &#75; | K   | 107 | 6B | 153 | &#107; | k   |
| 44  | 2C | 054 | &#44; | ,     | 76  | 4C | 114 | &#76; | L   | 108 | 6C | 154 | &#108; | l   |
| 45  | 2D | 055 | &#45; | -     | 77  | 4D | 115 | &#77; | M   | 109 | 6D | 155 | &#109; | m   |
| 46  | 2E | 056 | &#46; | .     | 78  | 4E | 116 | &#78; | N   | 110 | 6E | 156 | &#110; | n   |
| 47  | 2F | 057 | &#47; | /     | 79  | 4F | 117 | &#79; | O   | 111 | 6F | 157 | &#111; | o   |
| 48  | 30 | 060 | &#48; | 0     | 80  | 50 | 120 | &#80; | P   | 112 | 70 | 160 | &#112; | p   |
| 49  | 31 | 061 | &#49; | 1     | 81  | 51 | 121 | &#81; | Q   | 113 | 71 | 161 | &#113; | q   |
| 50  | 32 | 062 | &#50; | 2     | 82  | 52 | 122 | &#82; | R   | 114 | 72 | 162 | &#114; | r   |
| 51  | 33 | 063 | &#51; | 3     | 83  | 53 | 123 | &#83; | S   | 115 | 73 | 163 | &#115; | s   |
| 52  | 34 | 064 | &#52; | 4     | 84  | 54 | 124 | &#84; | T   | 116 | 74 | 164 | &#116; | t   |
| 53  | 35 | 065 | &#53; | 5     | 85  | 55 | 125 | &#85; | U   | 117 | 75 | 165 | &#117; | u   |
| 54  | 36 | 066 | &#54; | 6     | 86  | 56 | 126 | &#86; | V   | 118 | 76 | 166 | &#118; | v   |
| 55  | 37 | 067 | &#55; | 7     | 87  | 57 | 127 | &#87; | W   | 119 | 77 | 167 | &#119; | w   |
| 56  | 38 | 070 | &#56; | 8     | 88  | 58 | 130 | &#88; | X   | 120 | 78 | 170 | &#120; | x   |
| 57  | 39 | 071 | &#57; | 9     | 89  | 59 | 131 | &#89; | Y   | 121 | 79 | 171 | &#121; | y   |
| 58  | 3A | 072 | &#58; | :     | 90  | 5A | 132 | &#90; | Z   | 122 | 7A | 172 | &#122; | z   |
| 59  | 3B | 073 | &#59; | ;     | 91  | 5B | 133 | &#91; | [   | 123 | 7B | 173 | &#123; | {   |
| 60  | 3C | 074 | &#60; | <     | 92  | 5C | 134 | &#92; | \   | 124 | 7C | 174 | &#124; |     |
| 61  | 3D | 075 | &#61; | =     | 93  | 5D | 135 | &#93; | ]   | 125 | 7D | 175 | &#125; | }   |
| 62  | 3E | 076 | &#62; | >     | 94  | 5E | 136 | &#94; | ^   | 126 | 7E | 176 | &#126; | ~   |
| 63  | 3F | 077 | &#63; | ?     | 95  | 5F | 137 | &#95; | _   | 127 | 7F | 177 | &#127; | DEL |

Source: [www.LookupTables.com](http://www.LookupTables.com)

## Message Digest Schemes, such as MD5, and SHA (for NTP authentication)

### SHA 1 instead of MD5 authentication

#### Available Message Digests in at least version 5.4.5 and above

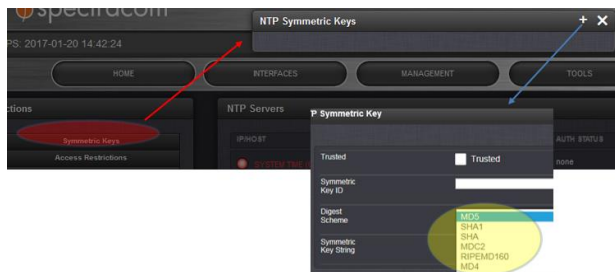
(**Note:** Not sure in what software version the others besides MD5 were added. I couldn't find it in the Release Notes. Believe it was after v5.12 and it was before version v5.4.5).

- This configuration is not available in the classic interface browser (have to use the newer black/charcoal browser)
- Selected in the **Management** -> **NTP setup** page of the newer browser:
  - Click on the “**Symmetric Keys**” button on the left side of the page. Then press the “+” sign in the upper-right corner of the pop-up window that opens:



**Email Keith sent (20 Jan 17)** The Spectracom SecureSync provides the ability to either select either MD5 or a different Message Digest schemes for NTP authentication. The below screenshot shows the available schemes

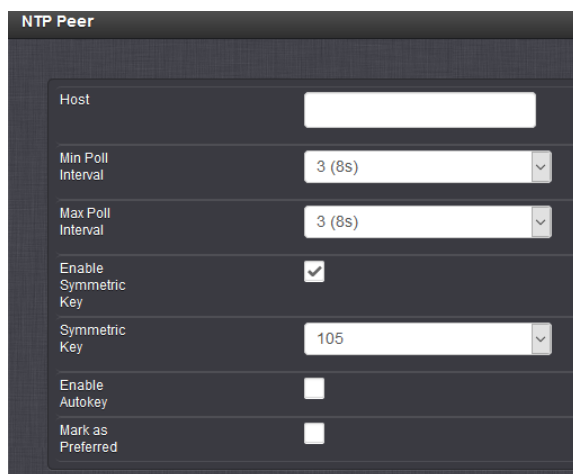
(in addition to MD5) that can be configured in the **Management** -> **NTP Setup** page of the SecureSync's web browser (click on the "**Symmetric Keys**" button on the left side of the page. Then press the "+" sign in the upper-right corner of the pop-up window that opens):



**Issue: "NTP Servers" table allowed symmetric key to be configured, but the "NTP Peers" table in the NTP Setup page did not allow symmetric key authentication (applicable to v5.4.4 and below only???)**

- At one time, SecureSync's NTP Servers table in the NTP Setup page allowed symmetric key to be configured, but the Peers table did not have this capability.
- Sometime prior to v5.5.1, symmetric key configuration had been added to the Peers table. I'm not certain, but after searching release notes, I believe this may have been added in version 5.4.5. The best inference I found to this change was in the 5.4.5 Release Notes: "[Corrected update/add/delete NTP Peer/Server line error](#)"

**Screenshot from 5.5.1 showing that at least v5.5.1 and above have this capability**



**Info regarding software versions prior to version 5.1.2**

- Refer to Mantis case 1990 <http://cvsmantis.int.rolia.com/mantis/view.php?id=1990>
- (12 Apr 2013) with at least Archive versions 4.8.9 and below, we only support NTP authentication using MD5 (we don't support using SHA1 or other hash generators). We don't provide access to the ntp keys file to switch to other mechanisms.
  - This is a limitation of the version of NTP we currently use (version 4.2.0).
- Version 5.0.0 upgraded NTP to v4.2.6P5, but did not add any changes to the web browser to be allow SHA1 to be selected. So it won't be available until sometime after Archive version 5.0.0.

**Update to this:** I believe this will be available in archive 5.1.2.

**Email from Paul Myers**

NTP technically supports MORE than MD5. SHA1/SHA may not be supported in NTP 4.2.0

Scnd email from Paul Myers

<http://lists.ntp.org/pipermail/questions/2011-December/031192.html>

On Thu, Dec 8, 2011 at 14:38, Joe Smithian <[joe.smithian@gmail.com](mailto:joe.smithian@gmail.com)> wrote:

> A,N,S, and M keys are defined in the man ntp.keys

>

> <http://www.gsp.com/cgi-bin/man.cgi?section=5&topic=ntp.keys>

That's a good example of why one should be suspicious of man pages for ntpd and friends -- the distribution docs are maintained as HTML and any man page variant is likely to be based on out of date information.

That page describes a ntp.keys scheme where the type column is always a single letter and it determines not only the digest algorithm, but also the representation. That's not how ntp.keys works today. The type column specifies only the digest algorithm, and only 'M' (or MD5) is supported prior to ntp 4.2.6. With 4.2.6 and later, the type column can specify the name of any suitable OpenSSL-provided digest algorithm which produces a 16-20 octet digest.

The format choice (between hexadecimal and ASCII) is driven by the length of the key value. If it is 20 characters or less, the ASCII is used directly as the key value. If it is 21 characters or longer, it is interpreted as hexadecimal-encoded.

Summary- SO FOR OUR NTP 4.2.0 ONLY MD5 works

---

**“Auth Status”**

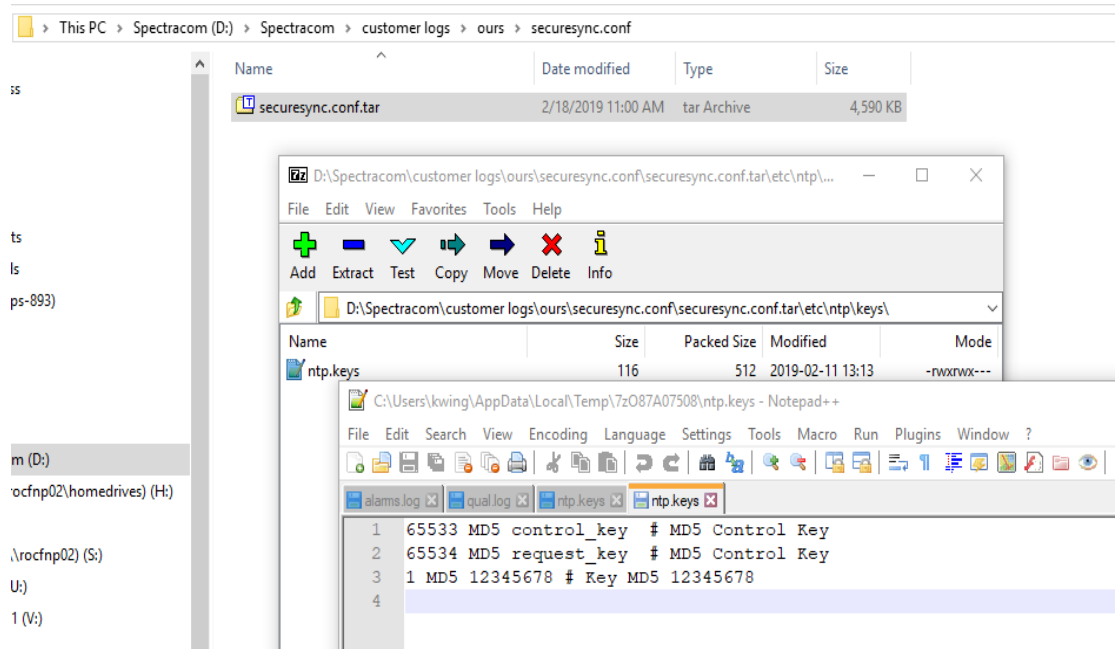
**Changing a Symmetric key after NTP has started-up.**

- NTP caches the symmetric keys when NTP starts-up. So if the key changes while NTP is running, the change isn't incorporated until NTP is restarted.
- The “Auth Status” will continue to report “ok” for authentication. But auth will fail in any other units polling this one, because NTP continues to authenticate each received packet. (NTP in other time servers will lose sync with that time server, if the key changes).

---

**Viewing/Backing-up/Cloning the Symmetric key file (“ntp.keys” file) via a config backup file.**

- Refer to Salesforce Cases such as **185548**
- (as of at least version 5.8.3) the ntp.keys file (Symmetric keys) **is** included in the exported config backup bundle (confirmed in v5.8.3 by Keith.on 18 Feb 2019, as shown below).
  - This means the **ntp.keys** file can be backed-up/viewed/cloned via the config bundle



**Note:** Info below about viewing/backing-up/cloning ntp.keys file has also been added a sub-section in the “**NTP Restriction and MD5 Authentication**” document (which can be sent to customers):  
[..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Restriction and Authentication-MD5 and SHA](#)

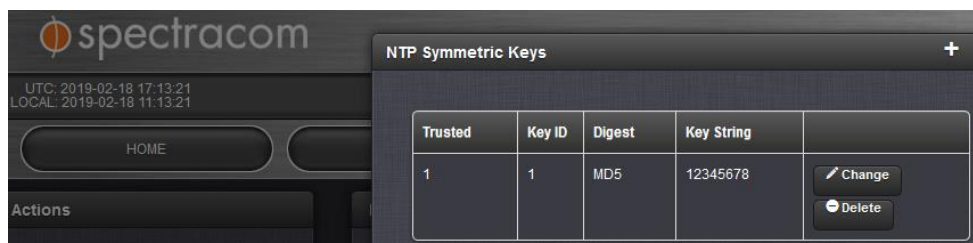
### Viewing the ntp.keys file (or to backup/clone the keys file)

- Refer to Salesforce Case 185794

Q We want to check the detail content dir /etc/ntp.keys as we need to enable and test secure NTP, but it's not working after we configure on client side, we plan to check the file after we configure secure keys on GUI, but our account do not have enough permission to view file dir /etc, please help.BTW. shall we have an account with root permission?

**A Reply from Keith (18 Feb 2019)** To begin, and for file integrity purposes, we DO NOT provide root access to SecureSyncs to anyone outside of our Engineering team. But Thanks for asking about this!

Secondly, the “**/etc/ntp.keys**” file cannot be viewed via SecureSync’s CLI interface. Within the SecureSync itself, the contents of the ntp.keys file can only be indirectly viewed, via the **Management -> NTP Setup** page of the web browser (then press the “Symmetric Keys” button on the left). The pop-up window of the “**NTP Symmetric Keys**” table will display the contents of the ntp.keys file (as shown below):



However, there is an alternate method to view the ntp.keys file directly (external to the SecureSync itself)...

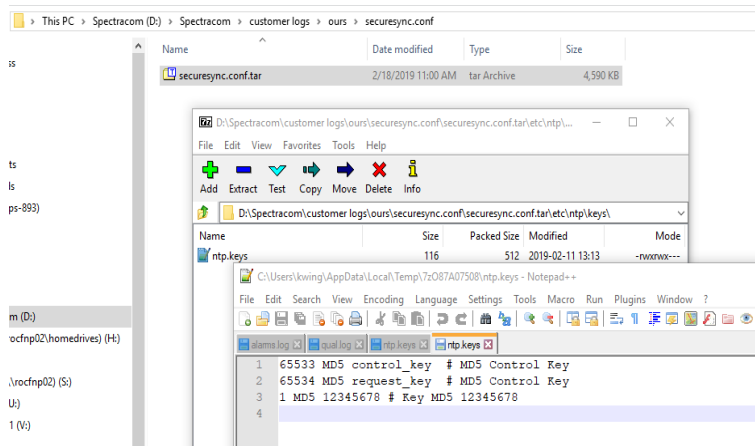
The ntp.keys file is included in the config backup bundle file, which is generated internally and can then be exported (using the web browser, or via an FTP/SCP CLI connection). This exported bundle file can be used to not only specifically view the contents of the ntp.keys file, but can also be used to backup most of the unit’s configs to a computer/clone SecureSyncs with similar configs (such as the NTP peers/servers tables, and symmetric key configs, for examples).



For info on backing-up/restoring (back into the same, or a different SecureSync) the config bundle file, please refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/ADMIN/ConfFilesBckpRest.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/ConfFilesBckpRest.htm)

Once exported (via the browser or CLI connection) the config bundle file is a “double-compressed” tar file. The exported file needs to be uncompressed (and the uncompressed file needs to be renamed as .tar and uncompressed again) before the files will be readable.

Once finally fully uncompressed, the raw ntp.keys file for the particular SecureSync, which the config file was exported, from will be viewable (as shown below):



## Troubleshooting Symmetric key auth not working

### 1. NTP Client not syncing with Authentication. Syncs just fine without Authentication

- Symmetric Keys don't match verbatim in the Client and Server
- NTP client's ntp.conf file has been edited, adding Access Control to the lines associated with the time server (such as **nomodify**)
- Use the View NTP Clients table to see which flags are being reported for that particular NTP client.
- Refer to sites such as: <http://support.ntp.org/bin/view/Support/AccessRestrictions>

### \*\*\*\*FIPS compliancy (FIPS 140-2) FIPS requirements for NTP- associated with NTP authentication)

- Refer also to FIPS info in: <..\CustomerServiceAssistance.pdf>

Review the network element configuration and verify that it is authenticating NTP messages received from the NTP server or peer using either PKI or a FIPS-approved message authentication code algorithm. **FIPS-approved algorithms for authentication are the cipher-based message authentication code (CMAC) and the keyed-hash message authentication code (HMAC). AES and 3DES are NIST-approved CMAC algorithms. The following are NIST-approved HMAC algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256.**

#### A) Examples of FIPS-compliant hashing algorithms

##### 1. PKI (Public Key Cryptography) such as NTP autokey

## 2. Cipher-based message authentication code (CMAC) such as AES and 3DES

- AES and 3DES are NIST-approved CMAC algorithms.

## 3. Keyed Hash Message Authentication Code (HMAC) such as SHA-1, SHA-2 and SHA3

- Refer to sites such as : <https://en.wikipedia.org/wiki/HMAC> and <https://www.oit.va.gov/Services/TRM/StandardPage.aspx?tid=5296>

The Keyed-Hash Message Authentication Code (HMAC), as described in Federal Information Processing Standards (FIPS) PUB 198-1, describes a HMAC mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative approved cryptographic hash function, in combination with a shared secret key.

- **NIST-approved HMAC algorithms include the following:** "SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256"

Hash algorithms for HMAC are Approved if they are listed in **FIPS 180-4** (or earlier versions). SHA-1, SHA-256 and SHA-512 are all FIPS Approved secure hash algorithms and the HMAC function based on them are thus FIPS Approved HMAC functions. Using a ...

**FIPS 180-4: Secure Hash Standard (SHS):** <https://csrc.nist.gov/publications/detail/fips/180/4/final>

## B) Examples of NOT FIPS compliant hash algorithms

### 1. MD5 authentication

- MD5 is not considered FIPS compliant (must use either SHA or SHA1)

per: <http://doc.ntp.org/4.2.6/authopt.html>

By default, the message digest algorithm is MD5 selected by the key type `M` in the keys file. However, if the OpenSSL library is installed, any message digest algorithm supported by that library can be used. The key type is selected as the algorithm name given in the OpenSSL documentation. The key type is associated with the key and can be different for different keys. The server and client must share the same key, key ID and key type and both must be trusted. **Note that if conformance to FIPS 140-2 is required, the message digest algorithm must conform to the Secure Hash Standard (SHS), which requires an algorithm from the Secure Hash Algorithm (SHA) family, and the digital signature encryption algorithm, if used, must conform to the Digital Signature Standard (DSS), which requires the Digital Signature Algorithm (DSA)**

## Viewing NTP authentication status (`ntpq -c associations` command)

there is a command you can issue from the SecureSync. This command will report all of the NTP associations connected to the SecureSync. This response provides an auth status column.

Connect to the CLI interface (via an SSH session, using the same login credentials as the web browser). Then type the following command `ntpq -c associations<enter>`

This command will not show which key is being used, but it will show that authentication is being done between the two NTP devices!!

The below Associations (AS) table is from: <http://doc.ntp.org/4.2.6/ntpq.html#clock>

| Variable   | Description                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------|
| ind        | index on this list                                                                                              |
| assid      | association ID                                                                                                  |
| status     | peer status word <span style="border: 1px solid black; padding: 2px;">See table below</span>                    |
| conf       | yes: persistent, no: ephemeral                                                                                  |
| reach      | yes: reachable, no: unreachable                                                                                 |
| auth       | ok, yes, bad and none                                                                                           |
| condition  | source (see peer status word)                                                                                   |
| last_event | event report (see peer status word) <span style="border: 1px solid black; padding: 2px;">See table below</span> |
| cnt        | event count (see peer status word)                                                                              |

The below table is at: <http://doc.ntp.org/4.2.6/decode.html#sys>

**Peer Status Word**  
The peer status word consists of four fields: Status (0-4, Select (5-7), Count (8-11) and Code (12-15). It is reported in the first line of the `ntpq` display produced by the `ntpq` program.

| Status                                                                                                                                                                                                                           | Select           | Count                             | Code                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------------------------------|------------------------------------------|
| The Status Field displays the peer status code bits in hexadecimal as follows:                                                                                                                                                   |                  |                                   |                                          |
| Code                                                                                                                                                                                                                             | Message          | Description                       |                                          |
| 01                                                                                                                                                                                                                               | host             | broadcast association             |                                          |
| 02                                                                                                                                                                                                                               | reach            | host reachable                    |                                          |
| 03                                                                                                                                                                                                                               | authen           | authentication enabled            |                                          |
| 04                                                                                                                                                                                                                               | auth             | authentication ok                 |                                          |
| 05                                                                                                                                                                                                                               | persist          | persistent association            |                                          |
| The Select Field displays the current selection status. The T Field displays the tally codes beginning the <code>ntpq</code> peers display. The values are coded as follows:                                                     |                  |                                   |                                          |
| Code                                                                                                                                                                                                                             | Message          | T                                 | Description                              |
| 0                                                                                                                                                                                                                                | not_selected     | -                                 | discarded as not valid (TEST0-TEST13)    |
| 1                                                                                                                                                                                                                                | not_selected     | -                                 | discarded by intersection algorithm      |
| 2                                                                                                                                                                                                                                | not_selected     | -                                 | discarded by table overflow (not used)   |
| 3                                                                                                                                                                                                                                | not_selected     | -                                 | discarded by the cluster algorithm       |
| 4                                                                                                                                                                                                                                | not_selected     | -                                 | included by the combine algorithm        |
| 5                                                                                                                                                                                                                                | not_selected     | -                                 | Backup (more than 120sec remote sources) |
| 6                                                                                                                                                                                                                                | not_selected     | -                                 | system peer                              |
| 7                                                                                                                                                                                                                                | not_selected     | -                                 | PPS peer (when the prefer peer is valid) |
| The Count Field displays the number of events since the last time the code changed. Upon reaching 15, subsequent events with the same code are ignored. The Event Field displays the most recent event message coded as follows: |                  |                                   |                                          |
| Code                                                                                                                                                                                                                             | Message          | Description                       |                                          |
| 01                                                                                                                                                                                                                               | assoclive        | association mobilized             |                                          |
| 02                                                                                                                                                                                                                               | assoclive        | association demobilized           |                                          |
| 03                                                                                                                                                                                                                               | serverunreach    | server unreachable                |                                          |
| 04                                                                                                                                                                                                                               | serverreach      | server reachable                  |                                          |
| 05                                                                                                                                                                                                                               | assocstart       | association restart               |                                          |
| 06                                                                                                                                                                                                                               | no_server        | no server found (ntpsec mode)     |                                          |
| 07                                                                                                                                                                                                                               | rate_exceeded    | rate exceeded (kiss code 300)     |                                          |
| 08                                                                                                                                                                                                                               | conn_refused     | conn refused (kiss code 100)      |                                          |
| 09                                                                                                                                                                                                                               | leap_rollback    | leap rollback from server LI code |                                          |
| 10                                                                                                                                                                                                                               | sys_peer         | become system peer                |                                          |
| 11                                                                                                                                                                                                                               | clock_error      | see clock status word             |                                          |
| 12                                                                                                                                                                                                                               | bad_auth         | authentication failure            |                                          |
| 13                                                                                                                                                                                                                               | popcorn          | popcorn spike suppressor          |                                          |
| 14                                                                                                                                                                                                                               | interleave_mode  | entering interleave mode          |                                          |
| 15                                                                                                                                                                                                                               | interleave_error | interleave error (recovered)      |                                          |
| 16                                                                                                                                                                                                                               | interleave_error | interleave error (recovered)      |                                          |
| 17                                                                                                                                                                                                                               | etc              | seconds values update from server |                                          |

**Note:** “Auth Status” is only updated when NTP first starts-up.

- “none”: Indicates authentication is not being used (no key has been specified in the specified peer/server in **Management** -> **NTP Setup** page)
- “bad”: Indicates authentication is being used, but the authentication failed when NTP last started-up
- Either no key ID or the wrong key ID may have been specified in the specified peer/server in Management -> NTP Setup page of one or more units.
- The selected key may not have been selected as “trusted” in the “Symmetric Keys” table

The selected key in the “Symmetric Keys” table may not match the same key in the other’s ntp.keys table

### Troubleshooting/ known issues with Symmetric key Authentication

#### B) NTP Authentication failures (“bad” or “none” instead of “ok”)

| NTP Peers                    |                |             |      |
|------------------------------|----------------|-------------|------|
| IP/HOST                      | REF ID         | AUTH STATUS | LAST |
| 10.133.12.150 (NOT IN SYNC)  | 172.30.133.149 | ok          | 1    |
| 172.30.170.150 (NOT IN SYNC) | 172.30.133.149 | bad         | 6    |

## “Auth Status”

**Note:** “Auth Status” is only updated when NTP first starts-up.

- “**none**”: Indicates authentication is not being used (no key has been specified in the specified peer/server in **Management** -> **NTP Setup** page)
- “**bad**”: Indicates authentication is being used, but the authentication failed when NTP last started-up
- Either no key ID or the wrong key ID may have been specified in the specified peer/server in **Management** -> **NTP Setup** page of one or more units.
- The selected key may not have been selected as “**trusted**” in the “Symmetric Keys” table
- The selected key in the “**Symmetric Keys**” table may not match the same key in the other’s ntp.keys table.

## Troubleshooting Auth failures

- With the original web browser design (versions prior to 5.1.0) do not use characters such as a “\$” (dollar sign). MD5 won’t work. (See note further below)
  1. Get the logs and especially the config files from both units.
  2. View the **ntp.conf** file from both units:

## C) Make sure the selected key is trusted on both units (as specified next to “trustedkey”)

**Example:** `trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534`

- 1) Make sure a key for each other (peers or servers) is selected and it’s the same number specified on both units.

Specific example below of where the customer only specified a key on one but not the other (notice the second red line does not contain the word “key” so the key hadn’t been specified in the Management->NTP Setup page. I had verified from both configs that both are supposed to be using key 2

### **mantp**

```
trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534
peer 10.133.12.150 key 2 minpoll 3 maxpoll 3
peer 172.30.170.150 key 2 minpoll 3 maxpoll 3 (auth was reported as “bad”)
server 172.18.33.191 key 2 minpoll 3 maxpoll 3
server 172.22.115.45 key 2 minpoll 3 maxpoll 3
server 10.153.36.191 key 2 minpoll 3 maxpoll 3
server 172.30.133.149 key 2 minpoll 3 maxpoll 3
keysdir /etc/ntp/keys/
```

### **sdcntp201**

```
trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534
peer 10.133.12.150 key 2 minpoll 3 maxpoll 3
server 172.18.33.191 key 2 minpoll 3 maxpoll 3
server 172.22.115.45 key 2 minpoll 3 maxpoll 3
server 10.153.36.191 key 2 minpoll 3 maxpoll 3
server 172.30.133.149 key 2 minpoll 3 maxpoll 3
peer 10.133.10.150 minpoll 3 maxpoll 3 (auth was reported as “none”) (notice the phrase “key 2” is missing from this line)
```

- 2) View the **ntp.keys** file in both config files to make sure the specified key matches verbatim the key of the other unit,

## Known issues/conditions with symmetric key authentication

### D) Issue with MD5 authentication not working with clients after updating from version 4.8.9 (NTP version 4.2.0) to versions 5.x.x (NTP version 4.2.6p5)

- Refer to Mantis case 2756 ([http://cvsmantis.int.rolia.com/mantis/view\\_all\\_bug\\_page.php](http://cvsmantis.int.rolia.com/mantis/view_all_bug_page.php))
- Also refer to Salesforce case 13501 for Paul Lindblad.
- Internal Knowledge article: <https://na8.salesforce.com/ka0C0000000L6H1>.
- He needed to edit Management -> NTP Setup, "Access Restrictions" after updating to archive version 5.x.x.

Our clients are now seeing the upgraded NTP server. I went to management /NTP setup/Access restrictions It seemed to be messed up. When I looked at it in the classic interface it looked OK. On the new GUI interface in the IP address column there were "-4"s I decided to change the IP in one column. When I did, all columns changed to that IP address. Then I tried to change the mask in one column. All columns changed to that mask. So I just deleted them all and manually typed the correct info in, one by one. This worked OK except for the fact that the IP version column kept wanting to say IPv6. I had to change this back to IPv4 on several of them. It seems stable now and the clients are seeing the NTP server.

### E) MD5 authentication not working with non-ASCII characters (Applicable to classic web browser design only, versions 5.0.2 and below)

**Note:** Update to at least version 5.1.2 (new browser) for non-ASCII characters.

In classic interface web browser- Do not use symbols such as the "\$" (dollar sign). The browser will accept the characters but it will prevent authentication from working at all. This is a limitation of the browser and not a limitation of NTP/MD5. Engineering believes the new web browser handles all characters correctly

### F) ntp peering not working. Ntp log contains

#### G) MAC decrypt: MAC length error

- Refer to Salesforce Case 192055
- Customer experiencing issues peering 5.8.2 SecureSync with a Solaris box running NTP (two Solaris boxes peered OK)
- **System log also contained:** [system] ERROR! NTP generic status polling: Ntpq error: 6 NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ\_UTIL\_STATUS) (STATUSD)
- might be related to NTP FIPS Mode as described in this article??  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=1442083](https://bugzilla.redhat.com/show_bug.cgi?id=1442083)

---

## Wireshark captures of NTP authentication

**Note:** In the following captures, 10.2.100.177 is the NTP server and 10.2.100.124 is the Client (using Presentense Client software)

### 1) NTP client not sending MD5 hash in its NTP request to NTP server (Client didn't send a hash)

```

1638 20:16:10.48793200 NTP 0 NTP Version 4, c1ient 10.2.100.124
<----->
[] Frame 1838: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
[] Ethernet II, Src: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49), Dst: Advantec_c9:04:6b (00:d0:c9:c9:04:6b)
[] Internet Protocol Version 4, Src: 10.2.100.124 (10.2.100.124), Dst: 10.2.100.177 (10.2.100.177)
[] User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
[] Network Time Protocol (NTP Version 4, c1ient)
 [] Flags: 0xe3
 Peer Clock Stratum: unspecified or invalid (0)
 Peer Polling Interval: 4 (16 sec)
 Peer Clock Precision: 0.000004 sec
 Root Delay: 0.0000 sec
 Root Dispersion: 0.0006 sec
 Reference ID: NULL
 Reference Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
 Origin Timestamp: Oct 27, 2015 20:15:55.484513000 UTC
 Receive Timestamp: Oct 27, 2015 20:15:55.489589000 UTC
 Transmit Timestamp: Oct 27, 2015 20:16:10.490678000 UTC

```

**Notice:**  
 No "Key ID" or "Message Authentication Code" is present below "Transmit Timestamp". The NTP time server will not include a hash in its response.

## 2) NTP client to NTP server sending key ID 2.

| No. | Time              | PTP_LLGI | Protocol | Peer Clock Stratum | VLAN | Info                  | Source       |
|-----|-------------------|----------|----------|--------------------|------|-----------------------|--------------|
| 487 | 19:28:21.83937700 |          | NTP      | 0                  |      | NTP Version 4, c1ient | 10.2.100.124 |

```

[] Frame 487: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
[] Ethernet II, Src: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49), Dst: Advantec_c9:04:6b (00:d0:c9:c9:04:6b)
[] Internet Protocol Version 4, Src: 10.2.100.124 (10.2.100.124), Dst: 10.2.100.177 (10.2.100.177)
[] User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
[] Network Time Protocol (NTP Version 4, c1ient)
 [] Flags: 0xe3
 Peer Clock Stratum: unspecified or invalid (0)
 Peer Polling Interval: 4 (16 sec)
 Peer Clock Precision: 0.000004 sec
 Root Delay: 0.0000 sec
 Root Dispersion: 0.0007 sec
 Reference ID: NULL
 Reference Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
 Origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
 Receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
 Transmit Timestamp: Oct 27, 2015 19:28:21.840073000 UTC
 Key ID: 00000002
 Message Authentication Code: b8a99f8310890a9a1c7322edbaee06

```

## 3) NTP server not able to authenticate (Key ID: 000000)

| Info                  | Source       | Source Port | Destination  | Length | Source Port | Destination Port |
|-----------------------|--------------|-------------|--------------|--------|-------------|------------------|
| NTP Version 4, c1ient | 10.2.100.124 |             | 10.2.100.177 | 110    | 123         | 123              |
| NTP Version 4, server | 10.2.100.177 |             | 10.2.100.124 | 94     | 123         | 123              |

```

[] Frame 488: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
[] Ethernet II, Src: Advantec_c9:04:6b (00:d0:c9:c9:04:6b), Dst: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49)
[] Internet Protocol Version 4, Src: 10.2.100.177 (10.2.100.177), Dst: 10.2.100.124 (10.2.100.124)
[] User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
[] Network Time Protocol (NTP Version 4, server)
 [] Flags: 0x24
 Peer Clock Stratum: secondary reference (2)
 Peer Polling Interval: 4 (16 sec)
 Peer Clock Precision: 0.000004 sec
 Root Delay: 0.0003 sec
 Root Dispersion: 7.9382 sec
 Reference ID: 10.2.100.44
 Reference Timestamp: Oct 27, 2015 19:38:18.362398000 UTC
 Origin Timestamp: Oct 27, 2015 19:28:21.840073000 UTC
 Receive Timestamp: Oct 27, 2015 19:38:24.472226000 UTC
 Transmit Timestamp: Oct 27, 2015 19:38:24.472415000 UTC
 Key ID: 00000000

```

**Notice:**  
 "Key ID" is all zeroes and no "Message Authentication Code" (MAC) is present in the NTP response if the Key ID and Message Authentication Code NTP response are NOT correct in the NTP time server (wrong key ID or wrong pass-phrase in the NTP server prevents successful authentication)  
 Note the NTP Clients MAC will be a different value in each NTP request

### C. NTP client to NTP server sending key ID 2

#### *NTP server successfully authenticated NTP client*

**Notice:**  
The "Key ID" is the same number as in the NTP request and the "Message Authentication Code (MAC)" is /resent/not all zeroes in the returned time stamp, if the Key ID and passphrase ARE correct in the NTP time server.  
Note the MAC in the NTP request and in the NTP response won't be the same value.

### \*\*NTP Autokey

- Refer to: <http://doc.ntp.org/4.2.4/authopt.html>
- Refer to (WP-033): <S:\Engineering\Projects\Lafayette\200 Engineering Documents\Working Papers>

Consists of both authentication and encryption

Can't be used in conjunction with symmetric key authentication

**NTP autokey Tech Note (in progress)** <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\NTPMD5 and Autokey Ap Note>

### Autokey stopped being supported in newer versions of NTP( 4.2.8p3 through 4.2.8p7)

- As of NTP v4.2.8p3 (update version 5.3.0 Sept 2015) NTP stopped supporting autokey

**Update:** NTP fixed Autokey in **version 5.4.5** (NTP v4.2.8p8) (this wasn't mentioned in the 5.4.5 release Notes, but I confirmed this with Ron, Joe and Dave S on 28 Sept 16)

### Example report from a version 5.4.1 customer:

"I'm having an issue enabling/configuring autokey for one of our SecureSync units. I've got it going on the other devices we have but for some reason I can't seem to get it configured properly on one of the units. I disabled NTP, went into the NTP config, checked the "enable" box, entered an appropriate passphrase, selected "trusted" for the certificate and clicked submit. At that point I go back into the configuration to get the GroupKey but it's always blank. When I try re-enabling NTP I get a "bad decrypt" error message (see below). I've tried rebooting the unit as well as re-applying the version 5.4.1 software. I've tried restoring the default NTP configuration as well but can't seem to get it to generate a GroupKey for the autokey. I'm at a loss for how to proceed. I've got this configured on three other devices, so I'm out of ideas at this point. I'd greatly appreciate any help."

- For more info on this condition, refer to NTP bug report [http://bugs.ntp.org/show\\_bug.cgi?id=3005](http://bugs.ntp.org/show_bug.cgi?id=3005)
- Version 5.3.0 update includes configs for autokey (we haven't removed them yet). But there are issues trying to use autokey starting with this version.
- As of Sept 2015, there is talk of autokey being replaced by something else, but no details available at this time
- See Ron Dries for questions about this.
- fixed in the version 5.4.5 software update. **Per email from Dave Sohn (29 Jul 16)** "Autokey in 5.4.1 is still not completely functional due to an issue within ntp itself. We just successfully tested autokey in ntp 4.2.8p8, which will be released with 5.4.5."

**Support for IPv6 Autokey:** Apparently, IPv6 Autokey is supported in the new version of NTP (4.2.6p5). If this is correct, since SecureSyncs with version 5.0.0 or higher have NTP v4.2.6p5, they should be compatible with IPv6. Refer to the link above for additional info on Autokey in this document.

---

### **\*\*Need to restart NTP after changing the Gigabit card configs**

- NTP needs to be restarted (or the unit rebooted), if the Gigabit Option Card (if installed) network port settings are changed. Otherwise, no NTP output on the ports.
- We aren't sure why this is. NTP must have some memory for storing this port info.

---

### **\*\*Time it takes for NTP to sync after power-up:**

- Version 4.7.0 change minpoll interval to "4 (16s)" for faster sync. The maxpoll is not specified, so according to Paul Myers, the poll interval is always every 16 seconds.

---

### **\*\*NTP Log entries**

- Refer to: NTP log entries

---

### **\*\*NTP's "LOCAL (0)" reference 127.127.1.0 (to allow NTP to go to stratum 16 when no inputs available) (aka "NTP Local Clock" reference)**

- 127.127.1.0 is the NTP Local Clock driver/reference used to cause NTP to go to Stratum 16 when the time server goes out of sync (exits holdover). This entry indicates NTP went to Stratum 16

### **Software versions 5.1.2 and above.**

#### **1. Archive versions 4.8.5 and below**

The local clock driver 127.127.1.0 is always enabled and always listed in the Status -> NTP page, NTP Reference Status table.

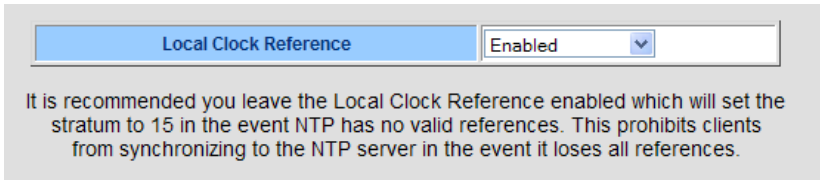
#### **2. Archive versions 4.8.6 to 4.8.9**

Local clock reference is used to allow NTP to be able to go to Stratum 16.

Version 4.8.6 added a field in the NTP Servers tab to enable or disable the Local Clock Reference (**Network -> NTP setup** page, **NTP Servers** tab)

In SecureSync/9400 series





### 3. In SecureSync/9400 series NTP Expert mode:

server 127.127.1.0 minpoll 4  
fudge 127.127.1.0 stratum 15

**In NTP log (when synced to Local Clock Reference):** ntpd[826]: synchronized to LOCAL(0), stratum=15

- When Local Clock Reference is enabled, allows NTP to be able to go to Stratum 16
- This reference is selected if no other inputs to NTP are available.

### 4. Archive versions 5.0.0 and above

NTP Local Clock Reference is now a dynamic reference that is only momentarily made available, as the SecureSync is going out of sync. Then the reference is removed, so that it can only be selected when SecureSync goes out of sync.

Appliance remaining at archive version 4.8.9 still shows reference ID "GPS"

NTP Selected Reference Status

| Sync | Host       | Ref ID | Stratum | LI | Mode   | Type  | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|------------|--------|---------|----|--------|-------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| 'o'  | System PPS | .GPS.  | 0       | 00 | Client | local | none        | 6          | 16                  | 377   | 0.000      | -0.008      | 0.002       |

Local clock still appears

NTP Reference Status

| Sync | Host         | Ref ID    | Stratum | LI | Mode       | Type    | Auth Status | Last (Sec) | Poll Interval (Sec) | Reach | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|--------------|-----------|---------|----|------------|---------|-------------|------------|---------------------|-------|------------|-------------|-------------|
| '*'  | System Time  | .GPS.     | 0       | 00 | Client     | local   | none        | 15         | 16                  | 377   | 0.000      | 0.001       | 0.002       |
| 'o'  | System PPS   | .GPS.     | 0       | 00 | Client     | local   | none        | 6          | 16                  | 377   | 0.000      | -0.008      | 0.002       |
| '*'  | 127.127.1.0  | LOCAL (0) | 15      | 00 | Client     | local   | none        | 16         | 16                  | 377   | 0.000      | 0.000       | 0.001       |
| '*'  | 10.35.19.100 | .PPS.     | 1       | 00 | Sym Active | unicast | none        | 34         | 64                  | 376   | 5.912      | -0.064      | 0.123       |
| '*'  | None         | ..        | 15      | 11 | Undef      | local   | none        | 0          | 0                   | 0     | 0.000      | 0.000       | 4000.000    |

Starting in Archive version 5.0.0, the Local clock reference is only periodically selected as the reference to NTP as the method to go to Stratum 16. The Local clock reference will no longer be displayed in the Status -> NTP page of the browser and the field to disable Local reference is no longer in the Network -> NTP setup page, NTP Servers tab. 127.127.1.0 is momentarily added to the NTP Reference table each time SecureSync exits Sync state. Then once NTP is Stratum 16, it's removed from the table. If a user happens to be viewing the NTP Status page when time sync is lost, and the page refreshes as the right moment, they may see 127.127.1.0 listed in the table. But shortly thereafter, they won't see it again, unless sync is regained and lost again.

The reason this was changed is because jittery inputs could result in NTP switching back and forth between our driver and the local driver. NTP would alternate between Stratum 1 and Stratum 16, even with the input always present. According to Paul, this newer method still lists the Local clock reference and fudge in the ntp.conf file (as was also done in the earlier versions of software). However, now NTP only periodically syncs to the local clock driver (instead of continuously) if System Time is not valid and no peers are available for sync.

Detailed info on this function. From Paul Myers (18 Dec 2013)

```

////////////////////////////////////
// Function Name: DT_FudgeNTP
// Description: This function uses NTPDC to use fudge to enable or disable
// a Local Reference Clock Driver to set the NTP Stratum to 15
// in the event NTP is not synchronized by the KTS with a
// reference or by a higher NTP Stratum server. The user

```

```

// can explicitly set a Local Reference Clock which disables
// this feature or explicitly disable it by putting a comment
// string in /etc/ntp/ntp.conf with the text
// # DISABLE_AUTO_LOCAL.
//
// The state machine for this system is shown below:
//
// .-----Restart NTP-----
// | |
// V |
// .----- Restart NTP.----- NTP Sync .-----
// | <-----| NTP Sync |<----- | NTP Out of|
// | NTP start | | Local Ref |----->| Sync Local|
// | or restart|----->| Clock off | NTP Out | Ref ON |
// `-----' NTP Sync `-----' of Sync `-----'
//
// The NTP Sync state disabled the Local Reference Clock
// if the user has NOT configured a Local Reference Clock
// line in ntp.conf or has not inhibited the feature of
// automatically enabling and fudging a local referenc clock
// when none is present in the ntp.conf file.
//
// If NTP goes out of sync, and NO local reference is defined and
// this feature is NOT inhibited, a Local Reference driver
// of stratum 15 is fudged. If NTP enters sync the Local
// Reference Clock driver is unconfigured.
//
// Parameters:
// In: None
// In/Out: None
// Out: None
// Returns: BOOL - Returns TRUE if fudging NTP
//
//

```

If desired, this function can be turned off using NTP Expert mode. More info on this from Paul Myers below.

To Disable Local Clock Reference in 5.0.0 and higher modify Expert mode file

Add line (to ntp.conf file):

```
DISABLE_AUTO_LOCAL
```

OR

```
127.127.1.0
```

Or actually add the local clock reference and fudge line

```
Server 127.127.1.0
Fudge 127.127.1.0
```

NTP log entry (versions 5.0.0 and above) asserted each time the Local Clock Reference is selected  
 ntpd[26487]: 127.127.1.0 interface 127.0.0.1 -> (none)

**Note:** the five digit number in brackets will vary.

## Causes of this NTP log entry being asserted

- 1) System Time no longer valid and no NTP peers have been configured.
- 2) System Time no longer valid and no configured NTP peers are available.
- 3) More than 3 or 4 NTP peers have been added and they are ganging up on the preferred System Time reference.

**Note:** This can cause NTP to disqualify all of its references, especially if the peers have high offsets from each other. If this happens, the NTP Status page may show that all references have an "x" to indicate they are not available for NTP to sync with.

---

## \*\*Automatic FTP of NTP Statistics

- This capability was available in the 9300s/9200s as part of the "Cachaça" project for South America.
- Not available in SecureSyncs/9400s in at least versions 5.8.5 and below (Sept 2019).

Q. Does the SecureSync/NetClock 9400 series have the option of send "Automatic FTP of Statistics", equal to 9300 series (every 30 minutes).

**A (as of 28 Aug 2013 per Keith)** No. This capability was not brought forward into the newer SecureSyncs. For your information, the NTP Statistics data is still available from the SecureSync and Model 9400s. It just not automatically sent out via FTP in the newer Models. Though it's not automatically sent out, it can still be easily retrieved via a single file of bundled logs.

The NTP statistics files that are sent out in the Model 9300s are the NTP Clockstats, Peerstats and Loopstats files. These files can be easily bundled into a single file, along with the other logs and then manually extracted whenever desired, using a manual FTP connection. The instructions below to do this are specific to SecureSync, but are very similar for NetClock 9400s as well.

In order to capture the log files, simply copy/paste all of the log entries (from all of the log tabs) in the SecureSync's **Tools** -> **Logs** page of its web browser (such as all of the log entries in the "Event" tab, "Alarms" tab, "Oscillator" tab, etc). Paste all of the log entries into a single Microsoft Word document and then send us this document for our review.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session. Then, simply attach this extracted file to a reply email. Below is additional information on how to bundle and extract all of the unit's logs:

Attached you will find an example log save file. In this Text document, you will find the Clockstats, loopstats and peerstats logs (just like with the Model 9300s). Just search this file for all three of these words.

---

## **\*\*NTP unicast / manycast / broadcast/ Multicast / NTP over Anycast**

### **NTP manycast mode**

- Refer to sites such as: <http://doc.ntp.org/4.2.0/manyopt.html>
- As of at least software version 5.2.1 (as of at least July 2015) NTP manycast mode is not supported via the web browser (but I suspect it's available via the NTP Expert Mode). Note there are not yet any tech notes available for this mode.
- We support NTP unicast, NTP broadcast, NTP multicast and NTP over Anycast modes only

What is NTP manycast (From <http://www.ntp.org/ntpfaq/NTP-s-config-adv.htm>)

This is an explanation by [Professor David L. Mills](#): "Manycast only works in multicast mode. It uses an expanding-ring search by adjusting the TTL field. This doesn't make sense in broadcast mode, since broadcast packets do not span subnets. It might in fact be useful to implement manycast in broadcast mode without the search, but that is rather far down the to-do list." (...) "Only the \* and + tattletales indicate a candidate survivor. Note that one of your servers is in process of going away, another coming onboard. This is a normal situation when first coming up and when the signatures are refreshed once per day. I assume you are using autokey; if not, no promises at all."

So basically it's a mechanism to automatically configure servers on a nearby network. Compared to broadcasting and multicasting, manycasting uses the normal server keyword, but with a multicast group address (class D) on the client. Manycast servers use the keyword manycastserver. As for broadcasts and multicasts, manycast associations on the client may come and go over time.

## NTP broadcast and NTP multicast

For broadcast and multicast troubleshooting/addition info, refer to: [NTP Broadcast/Multicast modes](#)

- NTP broadcast can be enabled without stopping/restarting NTP (starts broadcasting after being enabled)
- MD5 key needs to be defined, if the NTP client requires MD5 authentication.
- NTP Broadcast can be configured to go out all Ethernet ports if the Gigabit Card 1204-06 is installed (NOTE: Need to use NTP Expert Mode. Refer to the NTP expert mode tech note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast)
- NTP Multicast (224.0.1.1) only goes out one Ethernet port (the first network it sees as valid, such as Eth0 for instance (if its desired to multicast to more than on network, this has to be handled outside of the SecureSync).

**Note:** If the NTP client can configure which multicast address it monitors, the static routes in the main default gateway page can be configured for one multicast address to be sent out one specific network interface, while another multicast address can be sent out a different interface. We can multicast any IP address, so we can multicast 224.0.1.1 (the address reserved for NTP) on one interface (such as Eth1) and 224.0.0.1 (as an example) on a different interface (such as Eth2).

### H) NTP Broadcast Mode

#### Ability to configure the NTP Broadcast address

- Upgrade version 5.1.5 provides the ability for a user to configure the NTP broadcast address.
- The NTP broadcast address was statically set to the factory broadcast address in previous versions.

#### Management -> NTP Setup page of the newer browser

- Click on the gear icon next to “NTP Services”
- Click on the Broadcast tab

The screenshot shows the 'Edit NTP Services' configuration page. The 'Broadcast' tab is selected. The 'Enable Broadcast' checkbox is checked. The 'Broadcast Address' field is empty. The 'Broadcast Interval' is set to 3 (8s). The 'Enable Symmetric Key' checkbox is unchecked. Red arrows point from text boxes to these specific fields.

- Select this checkbox to enable Broadcast mode
- Broadcast address for the particular network
- Broadcast interval/rate to send NTP packets to the network's broadcast address

**Email Keith sent (20 Feb 17)** The SecureSync's Broadcast configuration provides the ability to configure the desired broadcast interval/rate. This is the rate at which NTP packets are sent to the broadcast address, with this rate determined by the requirements of the NTP clients requiring NT broadcast time stamps. the broadcast address that the packets are sent to is also configurable in this web page.

Both the network's broadcast address that the NTP clients are listening to for the NTP packets and the interval/rate which the packets are to be sent to this address have to be configured in the SecureSync which is broadcasting the NTP packets, in order for broadcast packets to be sent out of the SecureSync.

Note the value in parenthesis for each of the broadcast interval drop-down values is the actual interval for the packets to be sent. In the example screenshot above, the interval value of “3(8s)” indicates the NTP packets will be automatically sent to the defined broadcast address every 8 seconds. This is the fastest rate available, with the other available values sending the packets less often.

## Broadcastdelay (broadcast delay) value

Sets the typical propagation delay from this NTP server to the NTP clients receiving the NTP broadcast packets when broadcasting NTP (unlike when using unicast mode, the NTP clients can't calculate this propagation delay when using broadcast mode. So the NTP server can be configured to include/report this value in its broadcast packets).

“To compensate for any server-to-client packetlatency, you can specify an NTP broadcast delay (a time adjustment factor for the receiving of broadcastpackets by the switch)”

- This is a configuration associated with NTP broadcast mode, which is not currently available in the broadcast window of the newer web browser.
- Applicable to at least update versions 5.5.1 and below.
- Per Ron (21 Feb 17), He found NTP's default value is -50 milliseconds.
- This config value can be changed from -50ms by adding a line to the ntp.conf file via the NTP Expert mode (note that Expert mode must remain enabled, or this value will be removed from the ntp.conf file).

### Example ntp.conf file for adding broadcastdelay.

```
Server 127.127.1.0 # local clock
fudge 127.127.1.0 stratum 10
driftfile /var/lib/ntp/drift
broadcastdelay 0.008
keys /etc/ntp/keys
```

## Packet capture of NTP broadcast packet

|     |             |               |                |        |                                                         |                  |         |                 |               |
|-----|-------------|---------------|----------------|--------|---------------------------------------------------------|------------------|---------|-----------------|---------------|
| 438 | 10.7.508441 | 10.2.100.29   | 10.2.100.29    | Jabber | Response: Seq=100492                                    | Jabber           | Client  | From=10.0.1.100 | To=10.0.1.100 |
| 530 | 12.725603   | De11_6a:3e:32 | LLDP_Multicast | LLDP   | Chassis Id = 00:1c:23:6a:3e:30                          | Port Id = 1/0/24 | TTL = 1 |                 |               |
| 525 | 12.585466   | 10.2.100.20   | 10.2.255.255   | NTP    | NTP broadcast                                           |                  |         |                 |               |
| 441 | 10.269676   | 10.2.100.44   | 10.2.100.29    | Syslog | LOCAL7.NOTICE: spectracom: [system] AUTOMATIC D/A ADJUS |                  |         |                 |               |
| 328 | 7.508441    | 10.2.100.29   | 10.7.0.131     | TCP    | ms-wbt-server > psmond [ACK] Seq=100492 Ack=2676 win=64 |                  |         |                 |               |

**Email Keith sent to John Jenkins** To begin, configuring the SecureSync for NTP broadcast mode is extremely easy. In fact, you don't even need to stop and restart NTP in the process for it to start (many other NTP config changes require it to be restarted before the change takes effect).

To enable NTP broadcast mode, simply navigate to the **Network -> NTP setup** page of the browser, NTP Broadcasting tab. As shown below, change the “Broadcast Service” field to enabled and change the “Interval” drop-down to the desired broadcast interval (as indicated inside the parenthesis). Then hit Submit.

Note the “KEY ID” field should remain blank, unless the Harris equipment requires an MD5 authentication hash be sent with each NTP time stamp, in order for it to accept the time stamp. If MD5 is required (as it with many Cisco devices), let Dave or I know and we can tell you more about this particular configuration.

### NTP SETUP

General Settings
NTP Peers
NTP Servers
Symmetrical Keys
Autokey
NTP Broadcasting
NTP

|                          |         |
|--------------------------|---------|
| <b>Broadcast Service</b> | Enabled |
| <b>Interval</b>          | 4 (16s) |
| <b>Key ID</b>            |         |

4 (16s)

5 (32s)

6 (01mn04s)

7 (02mn08s)

8 (04mn16s)

9 (08mn32s)

10 (17mn04s)

11 (34mn08s)

12 (01h08mn16s)

13 (02h16mn32s)

14 (04h33mn04s)

15 (09h06mn08s)

16 (18h12mn16s)

17 (36h24mn32s)

After hitting Submit, the NTP packets will start to be transmitted at the interval specified. No other steps are required for them to go out. I just confirmed this with a wireshark capture, shown below. Wireshark capture is the best way to prove the time stamps are occurring. The packet(s) should indicate "NTP broadcast" originating from the IP address of the NTP server and going out to the broadcast address for the network.

|     |            |               |                |                                                                |
|-----|------------|---------------|----------------|----------------------------------------------------------------|
| 438 | 10.7.0.131 | 10.2.100.29   | 10.2.100.29    | Jabber / response: stratum= jabber-client from= root@respx     |
| 530 | 12.725603  | Dell_6a:3e:32 | LLDP_Multicast | LLDP Chassis Id = 00:1c:23:6a:3e:30 Port Id = 1/0/24 TTL = 1   |
| 525 | 12.585466  | 10.2.100.20   | 10.2.255.255   | NTP NTP broadcast                                              |
| 441 | 10.269676  | 10.2.100.44   | 10.2.100.29    | Syslog LOCAL7.NOTICE: spectracom: [system] AUTOMATIC D/A ADJUS |
| 328 | 7.508441   | 10.2.100.29   | 10.7.0.131     | TCP ms-wbt-server > psmond [ACK] Seq=100492 Ack=2676 win=64    |

Are there any switches or routers in between the NTP server and the Harris equipment? As this is broadcast traffic, switches/routers may or may not pass broadcast traffic.

Lastly, most if not all NTP clients will ignore the SecureSync's NTP packets if the SecureSync is not synced to either an external reference or to itself. To verify the SecureSync's NTP packets are useable, navigate to the **Status -> NTP** page of the browser. In the top row of this page is the current NTP Status. If the stratum value is a value such as 1 or 2, the NTP packets are useable. But if it indicates NTP is Stratum 16, the SecureSync is not in sync and the packets will likely be ignore by any NTP client. below is an example of NTP at Stratum 2. Its NTP packets are useable.

### NTP INPUT STATUS

Status
Time Offset
RMS Jitter
Frequency Offset

| Sync | Selected Reference | Stratum | LI | Delay (ms) | Offset (ms) | Jitter (ms) |
|------|--------------------|---------|----|------------|-------------|-------------|
| Yes  | 10.2.100.44        | 2       | 00 | 0.391      | 0.834       | 0.320       |

#### NTP broadcast on all four network ports (more than one isolated subnet)

- Scott will Larcan desired to broadcast NTP to all four subnets. Refer to Salesforce case 9886.
- Requires the use of NTP Expert mode (to add multiple NTP "Broadcast" lines to the ntp.conf file)
- Refer to the NTP Broadcast Tech Note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast to more than one port

Email I sent to Scott (17 May 2013)

Regarding the Spectracom SecureSync's NTP broadcast functionality; I have some information for you. I apologize for the delay in getting back to you (there are never enough hours in a day ☺)!!!

I started trying to log in to your SecureSync, but I was doing something wrong that prevented me from getting in. Before I could contact you about it, I got pulled off in a few other directions.

This morning, instead of looking at your SecureSync, I decided to test NTP broadcast on all isolated ports using one of our SecureSyncs here at the factory. This test went VERY well. I was able to confirm NTP is able to broadcast on every one of the four network ports, with each network port configured to be on different, isolated subnets.

I first did the same thing that you said you did- I enabled NTP Broadcast mode (every 16 seconds to speed up the test results) and then also NTP expert mode. In the ntp.conf table, I copy/pasted the "broadcast" line three times and edited each of the pasted lines to broadcast on three additional isolated subnets. Below is a copy of the edited ntp.conf file:

```

restrict 127.0.0.1
restrict -4 default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
broadcast 10.2.255.255 minpoll 4 maxpoll 4
broadcast 192.168.255.255 minpoll 4 maxpoll 4
broadcast 194.168.255.255 minpoll 4 maxpoll 4
broadcast 196.168.255.255 minpoll 4 maxpoll 4
server 127.127.45.0 prefer minpoll 4
enable pps
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
server 127.127.1.0 minpoll 4
fudge 127.127.1.0 stratum 15
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/

```

After editing the ntp.conf file, I then edited the IP addresses for Eth 0, Eth 1, Eth 2 and Eth 3 as follows:

**Eth 0**

| Version | IP Address   | Prefix | Delete | Info                   |
|---------|--------------|--------|--------|------------------------|
| IPv4    | 10.2.100.147 | 16     | na     | net mask = 255.255.0.0 |

**Eth 1**

| IP Version | IP Address  | Prefix | Delete | Info                   |
|------------|-------------|--------|--------|------------------------|
| IPv4       | 192.168.1.1 | 16     | na     | net mask = 255.255.0.0 |

**Eth 2**

| IP Version | IP Address  | Prefix | Delete | Info                   |
|------------|-------------|--------|--------|------------------------|
| IPv4       | 194.168.1.1 | 16     | na     | net mask = 255.255.0.0 |

**Eth 3**

| IP Address Setup |             |        |        |                        |
|------------------|-------------|--------|--------|------------------------|
| IP Version       | IP Address  | Prefix | Delete | Info                   |
| IPv4             | 196.168.1.1 | 16     | na     | net mask = 255.255.0.0 |

With the ntp.conf and Ethernet ports all configured, I then restarted NTP (**Network -> NTP Setup** page, **General Settings** tab)

Once NTP restarted, and with the SecureSync in sync (this is important, in order for NTP broadcast packets to be generated), I performed a wireshark capture on all four network connections.



Attached is a copy of each of the network port captures, showing NTP broadcast packets being successfully transmitted from the same SecureSync on each isolated subnet. The second value is the IP address for the SecureSync and the third value is the broadcast address configured in NTP, for that particular network port.

I'm not sure why you weren't receiving the NTP broadcast packets. Make sure that you restart NTP after editing NTP and the network port settings. Were you using Wireshark to capture the NTP broadcast packets, or seeing if your equipment was syncing to the packets? If you weren't using Wireshark to look for the packets, I definitely recommend you do so, especially if you try the steps above again and the equipment still doesn't sync sometime with the NTP broadcast schedule. Also make sure the Sync LED on the front of the SecureSync is green. Another good indication is the Stratum field in the first row of the Status -> NTP table should be a "1" (or a "2" if the SecureSync is synced to another NTPserver that is Stratum 1).

Please let me know that you see the NTP packets broadcast on all four networks.

## I) NTP Multicast mode

- Refer to NTP Multicast Tech note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast

### Desire to output NTP Multicast on more than one Ethernet port (Gigabit Option card installed)

- Refer to Salesforce case 9886
- This configuration won't work – Multicast NTP can only go out one Ethernet port (not more than one). So the gigabit card won't work for this application.

Unlike NTP broadcast which goes out on all network ports, NTP Multicast (224.0.1.1) only goes out one Ethernet port (the first network it sees as valid, such as Eth0 for instance). If it's desired to multicast to more than one network, this has to be handled outside of the SecureSync).

We recommended a dumb hub to repeat 224.0.1.1 on all output ports. Then use a firewall with port 123 left open, if it's desired to keep subnets isolated from each other.

## Configurations

NTP multicast settings are stored in the **stmd.conf** file (located in the **/config** directory) example entry below

```
spadmin@Spectracom ~/config $ cat stmd.conf
multicastAddress 239.0.0.1
portNumber 1024
messageId 1
spadmin@Spectracom ~/config $ █
```

---

## **NTP over Anycast mode** (aka “High Availability” or “HA”)

### Shortcuts/Refer to:

- Refer to SecureSync online user guide (“NTP over Anycast”): [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/NTP\\_Anycast.htm](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/NTP_Anycast.htm)
- Refer to “Spectracom Technology Brief” (on our website) [https://spectracom.com/sites/default/files/document-files/NTP\\_over\\_Anycast\\_TB12-101\\_revA.pdf](https://spectracom.com/sites/default/files/document-files/NTP_over_Anycast_TB12-101_revA.pdf)
- Link to data sheet on our website: <http://spectracom.com/documents/ntp-over-anycast>

### Testing NTP over Anycast mode (once its been configured)

- Document describing our NTP over Anycast test: [I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\NTP\NTP\\_Anycast mode](I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\NTP\NTP_Anycast mode)
- Refer to online SecureSync user guide (“Testing NTP over Anycast”) [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/AnyCast\\_Testing.htm](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_Testing.htm)
  - Note this test document is no longer posted on the website (“*Note: A detailed Anycast test procedure is available from Spectracom upon request. Please contact [techsupport@spectracom.oriola.com](mailto:techsupport@spectracom.oriola.com).*”)

### General info about NTP over Anycast

- First customer to beta test- Rachin Katti with Microsoft (Matt Loomis customer)
- Added to all SecureSyncs in software update **Version 5.2.0** (Feb, 2015). This feature is not available in software versions 5.1.7 and below.
- No license file is required. Automatically enabled in all SecureSyncs with 5.2.0 or above software.
- Anycast uses two assigned addresses. One is the unique, standard Unicast address and the other is a common Anycast address that all NTP slaves can be configured to point to.
- Anycast is a form of load balancing using a special routing protocol (OSPF). All NTP clients can be pointed to one static IP address. This simplifies network management, especially with many NTP clients on the network.

### below info excerpted from the online user guide:

#### What is NTP over Anycast (excerpted from online user guide):

[http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/NTP\\_Anycast.htm](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/NTP_Anycast.htm)

Anycast is a network routing protocol in which messages are routed to one of a group of potential receivers via a single Anycast address, thus avoiding the need to configure every client individually.

NTP over Anycast, as implemented in SecureSync, is a combination of the two concepts, allowing SecureSync to:

- Associate one of its network ports to an Anycast IP address, and
- Remove itself as an available time source if its reference is lost or degraded, and vice versa.

Please note that SecureSync utilizes the OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol).

- Refer to salesforce case 24570

Q Question Keith sent to Matt Loomis asking what High Availability was (based on a question from customer: have a second NTP unit coming that I would like to set up in **High Availability**).

**A Reply from Matt (28 Feb 17) Hi Keith,**

High availability is a terminology we are hearing more and more in the enterprise application space. Typically most of our customers looking for “high availability” usually are interested in NTP over AnyCast. But they could also be referring to a highly redundant setups with several failover options.....

You could check with Ron or Dave S if they have any additional input.

---

(Note: Below info is from our Anycast datasheet)

Refer to sites such as:

<http://en.wikipedia.org/wiki/Anycast>,

<https://www.pch.net/resources/papers/ipv4-anycast/ipv4-anycast.pdf>

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.116.6367&rep=rep1&type=pdf>

**What is Anycast** Anycast is a network addressing scheme in which messages are routed to one of a group of potential “receivers” via a single destination address based on a one-to-nearest association.

**NTP over Anycast** The NTP over Anycast feature is a combination of the time server’s ability to associate **one** of its network ports to an Anycast IP address and to remove itself as an available time source if there is a problem with its reference. As long as the time server is “in sync” it will be available for routing by OSPF to receive and respond to NTP requests. If the unit goes out of sync, it becomes unavailable. The request will be sent to the next nearest NTP server also configured with the NTP over Anycast address. In essence, it is the intelligence of the time server that removes the burden of this function from an NTP client so that the NTP client deployment can be simplified.

**Email from Matt Loomis (10 Aug 2016)**

Spectracom’s “NTP over AnyCast”: Each of the Stratum 1 servers are synchronized locally to their Stratum 0 GNSS reference source (GPS/GNSS). At the stratum 2 level, each of the Stratum 2 servers are clients to the Stratum 1 servers and peered to other Stratum 2 servers over unicast connections. The Stratum 2 servers are additionally setup with Anycast support to provide NTP to the application servers over Anycast connections.

This setup provides reliability at all levels. Stratum 1 servers that are out of sync or degraded will be flagged as false tickers by the Stratum 2 servers and will be removed from the NTP synchronization path until resolved. The Stratum 2 servers are also peered over unicast to other Stratum 2 servers for additional reliability. The application servers connect to the Stratum 2 servers, which are configured to support NTP over Anycast connections. This reduces the burden on the application servers, which connect to the shared Anycast addresses of the Stratum 2 servers rather than setting up to individual unicast addresses. If any of the Stratum 2 servers fall out of sync or are degraded, they are removed from the Anycast network, and different Stratum 2 servers on the Anycast network respond without any configuration changes required on the application servers.

Spectracom “NTP over Anycast” Video link:

<https://youtu.be/d5sSK2qV-ig>

“NTP over Anycast” Tech Brief link:

[http://spectracom.com/sites/default/files/document-files/NTP\\_over\\_Anycast\\_TB12-101\\_revA.pdf](http://spectracom.com/sites/default/files/document-files/NTP_over_Anycast_TB12-101_revA.pdf)

“NTP over Anycast” Diagram link:

[http://spectracom.com/sites/default/files/document-files/Hybrid%20Unicast-Anycast%20NTP%20Network\\_SD16-101%28A%29.pdf](http://spectracom.com/sites/default/files/document-files/Hybrid%20Unicast-Anycast%20NTP%20Network_SD16-101%28A%29.pdf)

**Email from Denis Reilly to Wai Fung with Bloomberg (2 Dec 2014)** We developed Anycast NTP in direct response to several customers who have asked for it. They wanted it because they wanted to make their NTP deployments in large systems easier. They wanted the ability to point all their NTP clients to a single IP address, and add and subtract server nodes without having to

reconfigure all of their clients (and specifically didn't want to use round-robin DNS).

There are other ways to accomplish this, both inside and outside of NTP. Brad Knowles is correct that NTP has extensive capabilities for failover. Those capabilities are a better fit for some deployments than Anycast would be.

We've found Anycast especially useful in large networks where the possible difference between GPS-synced time servers on the same IP address is small compared to the effect that the network will have on the time – but that assumes all Anycast servers are in sync. So we've also spent some time making sure that when our server loses its GPS reference, it "shuts off" the Anycast route, forcing clients to another (presumably in-sync) server. And there are other ideas we can implement to make Anycast better if customers continue to ask for improvements.

The feature is not officially released yet but it has done well in beta testing and (assuming no issues pop up) we plan on releasing it to all customers as part of the next SecureSync update, which should be delivered in January 2015. If you own a SecureSync, you can try it out for yourself at that point.

---

## Stub areas/NSSA stub

Q Does the appliance support stub areas? If no, how many routes can the routing table hold?

A **Per Ron Dries (22 June 2015)** We support nssa stub areas through expert mode configuration of the OSPF Anycast feature.

---

## Quagga account / quagga daemon

- Quagga is a new system account added in 5.2.0 to add NTP Anycast function to the black/charcoal browser (this account happens to be displayed in the classic interface. But since there is no password assigned to it. There is no way to use it for login. So there are no security issues with having it present. Customers should just ignore it.
- This unique user account is hidden in the newer black/charcoal browser but is exposed as an "artifact" in the classic interface browser (in at least version 5.2.0 and 5.2.1), since we aren't making changes to the classic interface.

**Email from Paul M (19 Mar 6)** These links describes anycast works and how to do it on Linux using a daemon that supports Anycast updates to external servers. This seems to be a robust way to implement Anycast support.

If this **Quagga** daemon is required, we would have to add it to SecureSync Gentoo Linux distribution.

<http://porky.linuxjournal.com:8080/LJ/187/10376.html>

<http://www.linuxsa.org.au/meetings/2006-07/anycast-dns.pdf>

<http://wiki.gentoo.org/wiki/Quagga>

---

## Default hello timer/dead timer

- **Hello timer:** 5 seconds
- **Dead timer:** 40 seconds

**Per Ron Dries (22 June 2015)** The default hello timer used in SecureSync is every 5 seconds. We typically use the default dead timer of the switch, which is 40 seconds. Other customers have done the same. The dead timer setting will determine how long clients will still be trying to query a server after it has stopped reporting a hello, so this can be configured for however sensitive you want the network to be.

---

## Ethernet Bonding (two IP addresses assigned to same port) / Link aggregation (LACP)

### A) Ethernet Bonding

**(email reply Keith sent about bonding in 2400 SecureSyncs Oct 2022)** I am not aware of port bonding/LACP being added in 1.6.0, and haven't heard of any specific plans/intentions to add it in a future update. There has been some limited discussions about it, but Port bonding is typically used for layer 1 packets (such as with routers/switches).

The SecureSyncs are a layer 2 application provider (not intended to be a switch/router), with active/backup fault-tolerance being inherently available within the time client software applications syncing to their NTP/PTP time servers (the client software application can be optionally configured to get time from more than one ethernet interface on the SecureSync. If an interface happens to become unavailable for some reason, it then inherently has immediate ability to receive its time stamps from another configured IP address/interface. This completely alleviates the need for port bonding/LACP.

## B) LACP

Q. The NTP Anycast is limited to one eth port. Can it be applied to more than one port through advanced routing somehow?

A Our web ui implementation supports NTP Anycast on a single Ethernet port. There is an expert mode configuration that allows the user to manually configure Zebra and OSPF protocols configuration files. This would allow them to configure Anycast on multiple Ethernet ports in the SecureSync had a Gigabit Ethernet option card installed. We have not tested this at this time. We recommend that Static IP addresses on separate networks would be used for any configurations.

Q.They want to have redundant eth ports on the SecureSync and mentioned LACP to allow them to have the same address on two ports to provide redundancy. Is this a feature that could be enabled somehow?

A reply from Paul Myers (30 June 15) We do not yet support LACP (Link Aggregation Control Protocol) at this time. I believe this would require some Linux kernel configuration and some changes to our software to support this. If desired can customer service enter a ECR (Engineering Change Request) describing the customer use case, customer opportunity to Product Management to be considered?

(11 Aug 15 KW) Per Dave Sohn, link Aggregation/Ethernet Bonding in SecureSync is feasible. It's just lower in priority right now.

---

**SecureSync utilizes the OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol).**

**\*\*Desire to use Cisco EIGRP (since OSPF not available)**

- Refer to Salesforce Case 230177 (April 2020)
- EIGRP is apparently a Cisco-specific protocol similar to OSPF.

**Email from Ron Dries to Keith (14 Apr 2020) from Case 230177:** The customer can still use NTP over Anycast, however in one of the switches it will have to take in the OSPF from the SecureSync and then redistribute it out across the network as EIGRP.

We do not have a VM version of SecureSync, they will need to have some device generating OSPF traffic and then configure the switch to take in OSPF and redistribute EIGRP. They can simulate OSPF traffic with a standard Linux VM on a PC, a package such as Quagga can be configured for OSPF in Linux, and then connect that PC/VM to a switch for testing and demonstration.

---

**\*\*eBGP (Border Gateway) protocol and OSPF NSSA feature (“OSPF Not-So-Stubby Area (NSSA)”)**

- Refer to RFC 1587 (<http://www.ietf.org/rfc/rfc1587.txt>)
- Anycast over the BGP protocol was added in software update version 5.4.1

**Summary: OSPF and BGP** are both protocols to help minimize management of NTP networks, by allowing all NTP clients to be configured with one same address that all NTP servers can sync with, no matter what the other IP Addresses are for that NTP server.

So if an NTP server needs to be swapped out or another NTP server is added, no reconfiguration of the NTP clients is necessary.

### Zebra (from Wikipedia)

**Zebra** is a routing software package that provides [TCP/IP](#) based routing services with routing protocols support such as [RIP](#), [OSPF](#) and [BGP](#). Zebra also supports special BGP Route Reflector and [Route Server](#) behavior. In addition to traditional [IPv4](#) routing protocols, Zebra also supports [IPv6](#) routing protocols. With [SNMP](#) daemon which supports [SMUX](#) protocol, Zebra provides routing protocol [management information bases](#).

Zebra uses an advanced software architecture to provide a high quality, multi server routing engine. Zebra has an interactive user interface for each routing protocol and supports common client commands. Due to this design, new protocol daemons can be easily added. Zebra library can also be used as a program's client user interface.

## A) eBGP (Exterior/External Border Gateway Protocol) (applicable only to versions 5.4.1 and above)

- NTP Anycast over the BGP protocol was added in software update version 5.4.1

From Wikipedia: [https://en.wikipedia.org/wiki/Border\\_Gateway\\_Protocol](https://en.wikipedia.org/wiki/Border_Gateway_Protocol)

**Border Gateway Protocol (BGP)** is a standardized [exterior gateway protocol](#) designed to exchange routing and reachability information among [autonomous systems](#) (AS) on the [Internet](#).<sup>[1]</sup> The protocol is often classified as a [path vector protocol](#) but is sometimes also classed as a [distance-vector routing protocol](#). The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a [network administrator](#) and is involved in making core [routing](#) decisions.

BGP may be used for routing within an autonomous system. In this application it is referred to as Interior Border Gateway Protocol, Internal BGP, or iBGP. In contrast, the Internet application of the protocol may be referred to as Exterior Border Gateway Protocol, External BGP, or EBGP.

---

## B) eBGP (External BGP) vs iBGP (internal BGP)

- Refer to sites such as: <https://supportforums.cisco.com/t5/lan-switching-and-routing/what-is-difference-between-ibgp-and-ebgp/td-p/708154>
- iBGP is formed between Neighbors within the same AS, whereas eBGP is formed between neighbors in different AS.

---

## C) BGP Authentication

- Refer to Salesforce Case Number case 191563
- Refer to JIRA ticket **SSS-632**
- not supported in at least v5.8.4 and below

**Excerpt report from case 191563 BGP Errors on Securesync (generated right after Anycast is enabled):**

```
2019/04/17 18:37:44 BGP: sockopt_tcp_signature: setsockopt(13): Protocol not available
2019/04/17 18:37:44 BGP: can't set TCP_MD5SIG option on socket 13: Protocol not available
```

If I remove the authentication from the route reflector and the clock's bgp config I do not see the errors and bgp establishes. Is bgp authentication supported?

---

## D) OSPF (Open Shortest Path First)

- OSPF for IPv4 was added in software version 5.2.0
- OSPF for IPv6 was added in software version 5.4.1
- In at least versions 5.7.1 we support OSPF v2 (IPv4) and OSPF (IPv6)

**From Wikipedia:** [http://en.wikipedia.org/wiki/Open\\_Shortest\\_Path\\_First](http://en.wikipedia.org/wiki/Open_Shortest_Path_First)

**Open Shortest Path First (OSPF)** is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

**Email from Rachin Katti (18 Nov 14)** We need OSPF NSSA feature enabled on the device. Our current network design doesn't align to area 0. Can you please let me know if this is something which can be done sooner? If yes, please share the timelines. Without this the NTP Anycast feature cannot be tested in our network. Thanks

#### excerpt from online user guide

```
OSPF Protocol EXAMPLE:

If an active SecureSync NTP server has removed itself as an available time source from the Anycast-capable network, the OSPF router will send a request for replacement to the next nearest NTP server, serving under the same NTP over Anycast address.

As soon as the first SecureSync server obtains a valid reference again, it will make itself available to the OSPF router, which will then use it as a time source again, based on the principle of shortest path available.
```

#### OSPF Type 1 and Type 2

- Refer to case 1889298 (Anycast working on SecureSync's immediate subnet, but not working through routers)
- Can use NTP over Anycast's dedicated Expert mode to change the default settings

Q Email from Dave Lorah to Apps team: ...they are configuring ANYCAST in the Securesync. They are having problems believed to be caused by the Securesync OSPF type. They say this is OSPF Type 2 and they need to use Type 1.

I think this is what they are referring to:

[https://www.juniper.net/documentation/en\\_US/junos/topics/concept/ospf-routing-external-metrics-overview.html](https://www.juniper.net/documentation/en_US/junos/topics/concept/ospf-routing-external-metrics-overview.html)

They mentioned a /etc/quagga/ospf/config in Cisco that can be edited to "redistribute connected metric – type 1" to change to type 1 in Cisco. Does the Securesync have this capability?

Additional question:

Can this be done through ANY CAST Expert mode?

```
Example ospfd.conf file:
*****|
router ospf
ospf router-id 10.2.100.157
network 10.2.0.0/16 area 0.0.0.0
redistribute connected
distribute-list default out connected
!
access-list default permit 10.10.14.1/32
```

access-list default deny any  
\*\*\*\*\*

**A reply from Pritam (8 April 2019)** OSPF by default will redistributed the network as type 2. If the user wants to redistribute as type 1, they have to specify in the redistribute command. something like this:  
*redistribute connected subnets metric-type 1*

**Note:** much of the following info/emails below is regarding Salesforce Case **210336**

In the link I sent you [http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_Anycast.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_Anycast.htm), on the right side under the NTP over Anycast heading are all the other links to general settings, OSPF IPv4, BGP, etc. It's a lot to put in one document so I sent a link to information which also links to other documents. You'll want to choose the setup instructions based on what you are using.

Q email from Jodi to Apps team: This customer plans to use NTP over Anycast, using OSPF IPv4.

Do you need an access port or a routed port?  
Does this need to be connected via a routing protocol? (I believe the answer here is yes)  
Is the shared IP a standard IPv4 address or a Multicast address? If the latter, is it self-assigned or do we need to provide one?  
Do only the clocks need to be within the multicast group or do all the end devices using them ALSO need to be within the same multicast domain?

Are these questions that we can answer, or are they in need of Prof Services to have us actually assist with configuring NTP over Anycast/their network?

**A Reply from Ron Dries (24 Oct 2019)** I think sending the customer the online manual and the tech brief from our website should help to answer most of their questions.

Here is a link to the main page in the manual which includes a link to the tech brief:  
[http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_Anycast.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_Anycast.htm)

If they have any follow on questions we can go from there.

The **Anycast address** is user configurable and a standard IPv4 address.

The only other configuration needed for OSPF IPv4 is which network port on the SecureSync they want to use and an OSPF area will need to be defined.

The SecureSync then informs the network using the OSPF routing protocol that it is a valid route to the configured Anycast address.

A network that has OSPF enabled will then propagate this information adding it to the routing tables of the switches that are in the same OSPF area.

It relies on the network settings of the ethernet port they choose to use, and the NTP traffic is routed to those network ports based on the OSPF information they receive saying they are valid routes to the configured Anycast address.

### **Altering the default Type Value (Type value 2 to Type value 1) using NTP Expert mode (Anycast tab)**

➤ **Refer to online SecureSync user guide**

[http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/AnyCast\\_ExpMode.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/AnyCast_ExpMode.htm)

**Email from Jodi (3 Dec 2019) pertaining to Case 210336** We believe that believe you leverage the **redistribute** command and add metric type line at the end to modify OSPF type1 or type2 route.



redistribute connected metric-type (1|2)

(Instead of “redistribute connected” that is what we default to in non-expert mode, which is type2--E2.)

We don't normally write scripts for this, but you may be able to find more information at: <https://www.quagga.net/> as well.

**Note:** the link above to the Anycast Expert section of the user guide provides some examples of how to edit the files.

---

## NTP over Anycast configuration/NTP Expert mode (Anycast tab)

### A) Configuring NTP Anycast via NTP Expert Mode (NTP Anycast button)

- Refer to online SecureSync user guide: [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/AnyCast\\_ExpMode.htm](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_ExpMode.htm)
- Allows ability for a user to directly edit the .conf files for Zebra, OSPF and BGP

**Per Ron Dries (3 Dec 2019)** “When they enable expert mode for anycast they are presented with the raw configuration files for quagga that they can manipulate.”

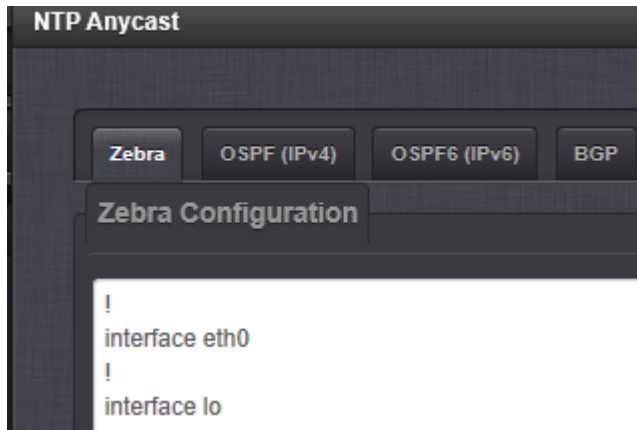
**B) \*\*Important note: the SecureSync MUST be in SYNC (either to itself, or to an external reference) for the NTP Anycast configurations to be able to be accepted**

**Note:** For example engineering software release testing of NTP over anycast mode, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 [https://app.bom.com/changes/detail-summary?change\\_id=2389346979](https://app.bom.com/changes/detail-summary?change_id=2389346979)) to find the PVP Test validation in the list of “ITEMS”

Example configs Engineering uses to test Anycast: [\\rocfnp02\ICS-Eng\Projects\Lafayette\300 Verification Test Plan\Regression Test\Anycast Configuration](#) (BGP is “zebra”?)

### Enabling/Accessing NTP Expert Mode for Anycast Expert

1. Navigate to the [Management](#) -> [NTP Setup](#) page of the browser
2. **Enable** NTP “**Expert Mode**” via Slider switch on left-side (if not already enabled)
3. Click the “**NTP Anycast**” button (top-left corner of the [NTP Setup](#) page, above the Expert mode switch)
4. With Expert Mode enabled, the NTP Anycast pop-up will now allow direct access to all four Anycast config files (via each of the four tabs at the top of the menu) as shown below:



- **Note:** the Anycast Expert section of the user guide ([http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/AnyCast\\_ExpMode.htm](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_ExpMode.htm)) provides some examples of how to edit the various Anycast config files.

### Config files for NTP over anycast

- zebra.conf, ospfd.conf and bgpd.conf are all located in /etc/quagga

```
spadmin@SpectracomCS176 /etc $ cd quagga
spadmin@SpectracomCS176 /etc/quagga $ ls
bgpd.conf ospf6d.conf ospfd.conf vtysh.conf zebra.conf
spadmin@SpectracomCS176 /etc/quagga $
```

### Example bgpd.conf file

```
spadmin@spectracomCS176 /etc/quagga $ cat bgpd.conf
!
router bgp 3
 bgp router-id 10.2.100.176
 network 10.2.0.0/16
 neighbor 10.2.100.192 remote-as 5
!
redistribute connected
!ips 10.2.100.192
spadmin@SpectracomCS176 /etc/quagga $
```

### Internal Type” or ”External Type 2” (How the SecureSync announces itself to the OSPF network)

- Refer to Case 210336 (Nov 2019)
- The “**Type**” value the SecureSync announces is not configurable or hard-set in the SecureSync
- Per Pritam, the “**Type**” is determined by the network.
- “Internal type” is announce when using OSPF Backbone Area 0.
- Otherwise, with any other Area, its announced as “**External type**”.
- Per the customer “We’re observing that the clocks are advertising that they are an External Type 2 and we need to have them advertise that they’re Internal.” Followed by “Internal would be best. External Type 1 would suffice (they’d at least be on the same playing field as other redistributed entities).”
- This value can apparently be hard-set in the SecureSync’s config files, via NTP Expert Anycast mode

**Email from Jodi (3 Dec 2019 for case 210336)** We believe that believe you leverage the **redistribute** command and add metric type line at the end to modify OSPF type1 or type2 route.

redistribute connected metric-type (1|2)

(Instead of “redistribute connected” that is what we default to in non-expert mode, which is type2--E2.)

We don't normally write scripts for this, but you may be able to find more information at:  
<https://www.quagga.net/> as well.

## Configuring NTP over Anycast via the web browser fields (not directly editing the conf files via NTP Anycast Expert Mode)

**\*\*Important note:** the SecureSync MUST be in SYNC (either to itself, or to an external reference) for the NTP Anycast configurations to be able to be accepted

**Note:** For example engineering software release testing of NTP over anycast mode, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 [https://app.bom.com/changes/detail-summary?change\\_id=2389346979](https://app.bom.com/changes/detail-summary?change_id=2389346979)) to find the PVP Test validation in the list of "ITEMS"

Example configs Engineering uses to test Anycast: [\\rocfnp02\ICS-Eng\Projects\Lafayette\300 Verification Test Plan\Regression Test\Anycast Configuration](#) (BGP is "zebra"?)

### Anycast configuration is broken into two "sections"

#### 1) The **FIRST** section is "General Settings" for Anycast mode (using OSPF or BGP).

- Refer to the online SecureSync user guide: <http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/AnyCastGenSets.htm>
- Refer to [http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP\\_Anycast.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_Anycast.htm)

**about the Anycast Address (for both OSPF and BGP modes):** this is a unique static address assigned to just one specified interface port as a "software" port for NTP clients to sync with. This address is only accessible when Anycast is configured correctly and running.

This address does not need to be on the same subnet as the physical address. This address is assigned as an "LO" (local interface) for the physical port.

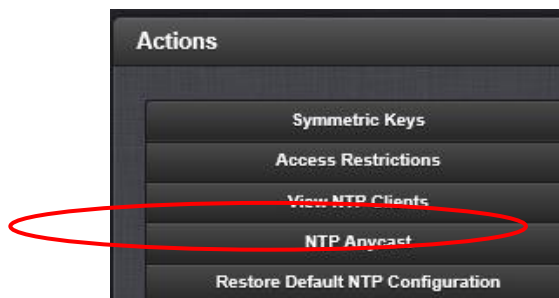
This address does not need to be manually configured anywhere except within the SecureSync and the NTP clients. The SecureSync advertises it to its switch, and the switch adds this address to its routing table

**Note:** A troubleshooting tip is to look at the switch's routing table to see if the Anycast address is listed in this table. If NTP anycast is configured and RUNNING, it should be in this routing table.

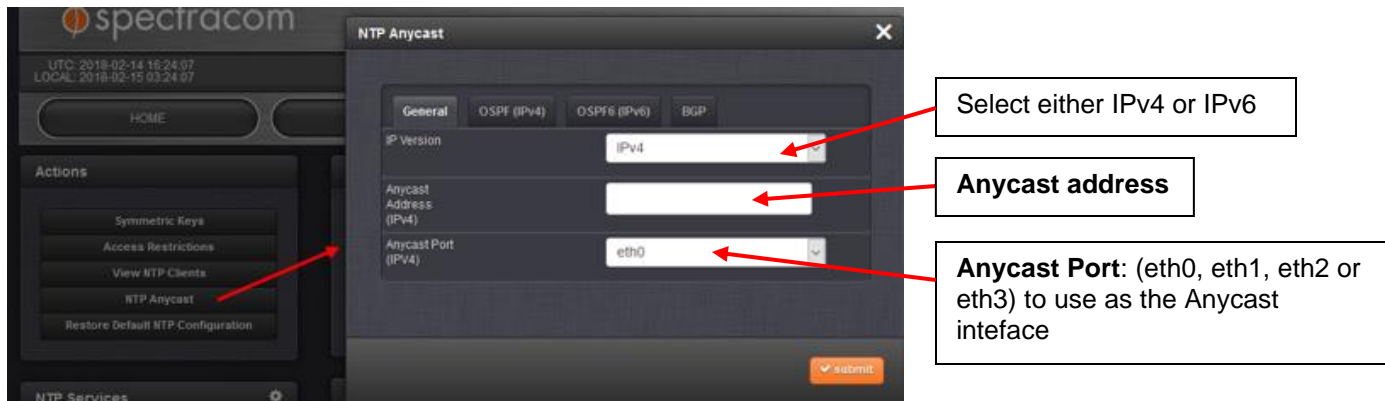
This address should be limited to a "private" address per RFC 1918 (not a public address that is reserved for the Internet (unless it's a closed network and customer is aware that this address must remain "internal" to their private network.

### To setup the NTP over Anycast functionality:

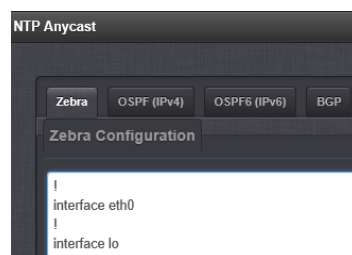
1. Confirm that your existing network infrastructure is **Anycast capable**. Determine network specifics, such as the Anycast address and port.
2. In the SecureSync Web UI, navigate to MANAGEMENT-> NTP Setup page
3. In the "Actions" Panel (left side of the screen), click "NTP Anycast".



- In the NTP **Anycast** window, select the **General** tab.



**Note per Keith (Oct 2019)** as shown below, if the **"General"** tab is not displayed (and a **"Zebra"** tab is present) make sure **NTP Expert mode is OFF** (left side of the NTP Setup page)



- Select the IP Version you will be running Anycast service for. The options are IPv4, IPv6, or both.
- Configure the **Anycast Address** to be used.

**Note:** only one (1) Anycast Address can be selected/available for the NTP clients to get time from

- Anycast Port:** choose the desired interface ("eth0" if 1204-06 card not installed, or can also select eth1, eth2 or eth3 if the 1204-06 Option Card is installed) to associate the Anycast service with.

**Note:** the Web browser only allows one (1) particular interface be selected as the Anycast port for NTP clients to get time from. But apparently, more than one interface port can be configured, if NTP Expert mode is enabled (**Management** -> **NTP Setup** page of the browser)?

**Email from Pritam to Jodi (28 Jan 2020)** "is customer trying to use more than 1 ethernet port ? If yes then they have to set up using NTP Expert mode to add multiple ports. WEB-UI only allows to bind 1 ethernet port for anycast NTP"

If you desire IPv6 functionality, you must also select the IPv6 port address since there may be multiple IPv6 addresses on a single port.

- Click Submit.

- 
- 2) The **SECOND** section for NTP Anycast Configuration is specific configuration for either **OSPF** or **BGP** modes

Refer to the online SecureSync user guide:

- 1) Specific configuration for OSPF mode is in online guide:

<http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/AnyCastOSPFv4.htm?Highlight=ospf>

- Refer to “**A**” further below

OR

- 2) Specific configuration for **BGP** mode is in online guide applicable only to versions 5.4.1 and above) [http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/AnyCast\\_BGP.htm](http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/AnyCast_BGP.htm)

- Refer to “**B**” further below

Now Proceed to either:

“**A**” below for **OSPF** mode

OR

“**B**” further below for **BGP** mode

#### A) OSPF protocol (applicable to software versions 5.2.0 and above)

- <http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/AnyCastOSPFv4.htm?Highlight=ospf>

Q Does the SecureSync contain any internal OSPF tables such as the OSPF routers have? If so what is the capacity and will a large table slow down performance? Are there any limits to these table sizes?

Q Another similar question (SF case 118310) How many routes can the routing table/OSPF DB hold in the SecureSync?

A I told him the SecureSync does not keep track of that and it is done in the routers but he disagreed so I said I would check.

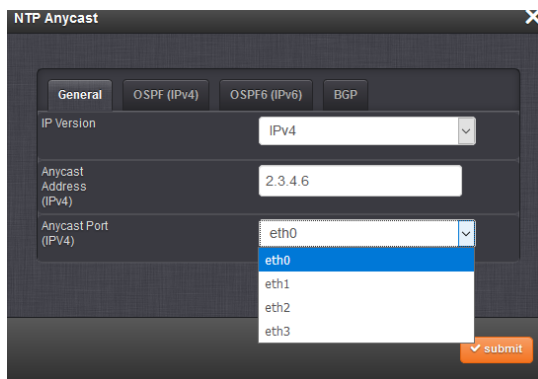
A Follow-up reply from Paul Myers (30 June 15) Our configurations of Zebra and OSPF simply setup an Anycast Interface configuration. We do not configure the SecureSync as an OSPF Anycast Router. We participate as an endpoint in the Anycast network architecture. Zebra and OSPF collaborate with the Anycast Router using OSPF to update the routing table to let us participate in using the defined Anycast address.

#### A.1 Configuring in software versions 5.4.0 and above (refer to “B.2” further below for versionz5.3.1 and below)

1. **Management** -> **NTP Setup** page of the browser and click on **NTP Anycast** (button on the left side of the page)



2. Select the **General** tab to configure the NTP Anycast port and Anycast address



**Anycast address:** common static address (not a unique “pre-set” value)

**OSPF port:** Which one of our Ethernet interfaces communicates with the OSPF switch.

3. Select either the “**OSPF (IPv4)**” or (**OSPF (IPv6)**” tab (as applicable) to enable NTP over Anycast and to configure the OSPF area



**Enable:** Enables Anycast mode

**OSPF area:** (AKA the “backbone area, area 0 or area 0.0.0.0). It’s the IP address of a main router in an area

### “Internal Type 2” or “External Type 2” (How the SecureSync announces itself to the OSPF network)

- Refer to Case 210336 (Nov 2019)
- The “**Type**” value the SecureSync announces is not configurable or hard-set in the SecureSync
- Per Pritam, the “**Type**” is determined by the network.
- “Internal type” is announce when using OSPF Backbone Area 0.

- Otherwise, with any other Area, its announced as “**External type**”.
- Per the customer “We’re observing that the clocks are advertising that they are an External Type 2 and we need to have them advertise that they’re Internal.” Followed by “Internal would be best. External Type 1 would suffice (they’d at least be on the same playing field as other redistributed entities).”
- This value can apparently be hard-set in the SecureSync’s config files, via NTP Expert Anycast mode for Quagga.

**Email from Jodi (3 Dec 2019 for case 210336)** We believe that believe you leverage the **redistribute** command and add metric type line at the end to modify OSPF type1 or type2 route.

redistribute connected metric-type (1|2)

(Instead of “redistribute connected” that is what we default to in non-expert mode, which is type2--E2.)

We don’t normally write scripts for this, but you may be able to find more information at: <https://www.quagga.net/> as well.

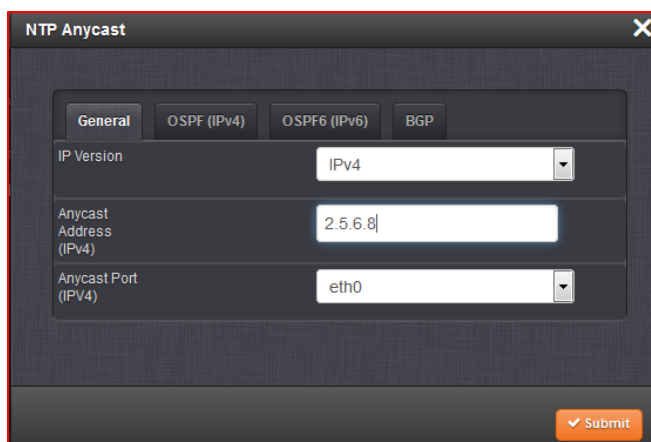
## B) BGP protocol (applicable only to versions 5.4.1 and above)

- [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/AnyCast\\_BGP.htm?Highlight=bgp](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_BGP.htm?Highlight=bgp)

1. **Management -> NTP Setup** page of the browser and click on **NTP Anycast** (button on the left side of the page)



2. Select the **General** tab to configure the **NTP Anycast interface** and **Anycast address**



**Anycast address:** common static address (not a unique “pre-set” value)

**OSPF port:** Which one of our Ethernet interfaces communicates with the OSPF switch.



3. Select the **BGP** tab to **enable BGP** as well as configure **AS Number** and **Neighbor info**

NTP Anycast

General OSPF (IPv4) OSPF6 (IPv6) **BGP**

Enable BGP

AS Number

Neighbor Address (IPv4)

Neighbor AS

Make sure the **AS Number** (assigned to the SecureSync) and **Neighbor AS** (configured in the SecureSyncs immediate switch) are not the same value.

Note the values for the **Neighbor Address** and **Neighbor AS** fields are obtained from the immediate switch connected to the defined Anycast interface of the SecureSync (such as eth2 for instance) as defined in the General tab)

**AS Number:** unique identity value assigned to the SecureSync (cant be the same as the “Neighbor AS” value)

**Neighbor Address** obtained from the next network device (the switch the SecureSync is connected to) This is not info about any other NTP server on the network.

**Neighbor AS:** unique identity value for this next network device (usually the switch the SecureSync is connected to) as obtained from that device. This is not info about any other NTP server on the network.

*(at least v5.8.9) Software issue with Enable BGP checkbox remaining selected until toggling NTP off/on*

- Refer to Salesforce Case 252845 (~Nov 2020)

**Per Dave Lorah:** Continued experimentation allowed me to find an apparent bug in the software so far.

If the BGP Enable checkbox is checked and submitted, it will remain checked until NTP is toggled off/on. If you do, you must go check the BGP Enable box again afterwards.

I find it does persist over a reboot but not sure over a power off/on.

I have submitted this to engineering as a bug report. We will investigate and have this fixed in a future firmware release.

### Multiple peers and more than one BGP neighbor

Customer wants to be able to **use multiple peers** and define **more than one BGP neighbor** with NTP Anycast. Does this need a JIRA ticket? Is this an enhancement request?

- Refer to [JIRA ticket SSS-722](#) for the email below (feature add to allow multiple peering for Anycast BGP using WEB-UI)

Q about neighbors (from Case 210710) It appears that gui only allows for one bgp neighbor relationship. Is there a way to configure BGP to multiple peers?

**A Reply from Jodi based on email from Pritam (16 Oct 2019)** I reviewed this with an Engineer yesterday. Potentially, you can use NTP Expert Mode of NTP Anycast, with great caution, to add more BGP neighbors. You would write directly into the Anycast configuration files (bgpd.conf).

Expert Mode should be utilized by advanced users, as incorrectly altering the Anycast files can cause Anycast to STOP WORKING. Also, any configurations made in Expert Mode will be lost as soon as Expert Mode is disabled, please note.

Once you configure one BGP neighbor, and switch to Expert Mode, you should be able to duplicate the configuration for

more neighbors. If you cannot, or this produces an error, we need to request an enhancement for you to be able to do this. If you feel comfortable using Expert Mode, and have thoroughly read the information and instructions at the link below, let us know.

[http://manuals.spectracom.com/NC/Content/\\_Global/Topics/NTP/AnyCast\\_ExpMode.htm](http://manuals.spectracom.com/NC/Content/_Global/Topics/NTP/AnyCast_ExpMode.htm)

### C) Requirement to use MD5 Authentication with NTP over Anycast (either OSPF or BGP)

- Refer to Salesforce Case 225867 (March 2020)
- For info on using Expert Mode, refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/AnyCast\\_ExpMode.htm?Highlight=ospf](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_ExpMode.htm?Highlight=ospf)
- The factory browser settings do not allow MD5 Authentication (nor are there any intentions to add it), but it can be configured using the **NTP Expert mode** settings for OSPF/BGP.

Q I'm standing up another SecureSync host and I'm going to be doing OSPF Anycast peering with a Cisco IOS host that requires MD5 authentication with the OSPF

**A Email Keith sent for Case 225867 (March 2020)** I hadn't come across this requirement for MD5 Authentication with OSPF before, so I checked with our Apps Engineering team. They informed me that the "standard" SecureSync's web browser interface for OSPF doesn't provide the ability to configure MD5 authentication.

However, there is an available "Expert Mode" for OSPF, which provides the means of configuring OSPF for other "less typical" settings (besides the factory-provided settings in the Standard OSPF browser pages) such as for MD5 authentication.

For more info on enabling/using the available Expert mode for OSPF, please refer to the online SecureSync user guide at: [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/AnyCast\\_ExpMode.htm?Highlight=ospf](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_ExpMode.htm?Highlight=ospf)

For more info on configuring MD5 for OSPF, refer to sites such as: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13697-25.html> and <https://networklessons.com/ospf/how-to-configure-ospf-md5-authentication>

### D) B.2 Configuring OSPF in Software versions 5.3.1 and below (refer to info above for versions 5.4.1 and above)

1. **Management** -> **NTP Setup** page of the browser and click on **NTP Anycast** (button on the left side of the page)



I confirmed my understanding with Denis Riley but will also ask Artem and CC Ron who is out on vacation if OSPF uses large internal tables.

**Enable:** Enables Anycast mode

**Anycast address:** common static address (not a unique "pre-set" value)

**OSPF area:** (AKA the “backbone area, area 0 or area 0.0.0.0). It’s the IP address of a main router in an area

**OSPF port:** Which one of our Ethernet interfaces communicates with the OSPF switch.

### **Any internal routing**

Q Does the SecureSync contain any internal OSPF tables such as the OSPF routers have? If so what is the capacity and will a large table slow down performance? Are there any limits to these table sizes?

A I told him the SecureSync does not keep track of that and it is done in the routers, but he disagreed so I said I would check.

**A reply from Paul Myers (30 June 15)** Our configurations of Zebra and OSPF simply setup an Anycast Interface configuration. We do not configure the SecureSync as an OSPF Anycast Router. We participate as an endpoint in the Anycast network architecture. Zebra and OSPF collaborate with the Anycast Router using OSPF to update the routing table to let us participate in using the defined Anycast address.

---

## NTP over Anycast Operation/Testing

### Testing NTP over Anycast mode (once its been configured)

- Document describing our NTP over Anycast test: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\NTP\NTP Anycast mode>
- Refer to online SecureSync user guide (“Testing NTP over Anycast”) [http://manuals.spectracom.com/SS/Content/\\_Global/Topics/NTP/AnyCast\\_Testing.htm](http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_Testing.htm)

### General info (OSPF and BGP)

#### 1. OSPF

Each time a OSPF-configured SecureSync goes into sync/NTP Stratum 1, its OSPF daemon starts-up to start sending ‘Hello’ messages to the OSPF switches. It also sends a routing message to the switch. The OSPF switch(es) on the network then knows all the routes to its OSPF-configured SecureSyncs.

As long as each OSPF-configured SecureSync remains in sync and NTP is still in sync, the OSPF daemon will continue to send ‘Hello’ messages every 10 seconds, to let the switch(es) know that it’s still an available OSPF route that can be used for NTP client requests.

When there are various subnets (varying number of hops between clients and the NTP servers) more than one NTP server may be actively receiving NTP requests from NTP clients in its “area of the network”. The other servers with longer routes just don’t receive any NTP packets if other servers are closer and still sending their ‘Hello’ messages every 10 seconds.

If the SecureSync initially goes into Holdover and then out of sync, the OSPF daemon is stopped, causing the Hello messages to stop being sent out. The OSPF switch has a configurable “dead timer” delay for when the Hello messages stop to when it stops routing NTP requests to that SecureSync. As there can be a delay between loss of sync and when the next Hello message is sent (in addition to the dead-timer delay in the switch), there may still be NTP time requests sent to the unsynced SecureSync. These NTP requests do not get re-routed to another NTP server. NTP just drops the time stamp as it usually does when OSPF isn’t being used. The client will just request time again at its next poll interval,

#### 2. BGP

- Ron Dries says SecureSync handles it internally the same way. But the network routing is handled differently.
- Per <https://networklessons.com/bgp/bgp-messages>, Apparently, the two BGP devices (secureSync and Switch) first perform a tcp handshake before performing any BGP packet exchanges.

---

### Log entries associated with NTP over Anycast mode

- Review the Daemon log for OSPF/Zebra entries (refer to troubleshooting Anycast further below)

#### Journal log entries for OSPF

- Refer to Mantis case 3223
- In at least version 5.3.1 (and 5.4.0) it appears Anycast config changes aren’t being logged in Journal log.

---

### SecureSync internally re-routes NTP packets based on health of NTP

- Re-routing of NTP requests when NTP is not healthy (The Server is not synced and NTP is Stratum 16) is handled internal to the SecureSyncs (not handled by the network).

---

**Desire to use OSPF for load balancing of thousands of NTP requests per second**

- NTP over Anycast functionality is not a load balancer
- This function cannot be used as a network load balancer to increase the number of NTP requests per second that time servers can respond to each second (the SecureSyncs cannot re-route NTP requests to another NTP server if NTP is dropping packets because its capacity each second has been exceeded).

# Troubleshooting NTP over Anycast not working (clients can't sync to the Anycast address)

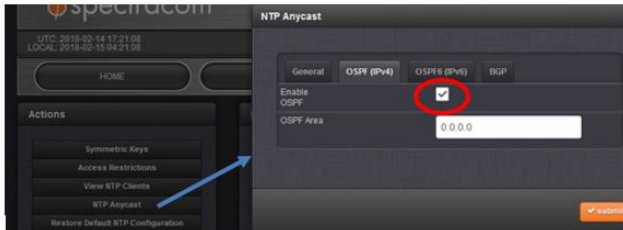
## A) General troubleshooting

1. Verify the single configured/dedicated **Anycast address port** is connected to the network with the NTP slaves (anycast works only on the specific configured interface (and no others). As configured in the **Management -> NTP Setup** page, **NTP Anycast** button (left side of page). Then select the **General** tab



- A) Verify that this interface is on the network with the NTP clients (this is the only interface which will work with the NTP Anycast address)
  - B) Make sure this selected network interface port is reachable on the network (via its assigned "physical" IP address/hostname)
  - C) Verify NTP slaves can successfully sync when configured with the IP address of this physical interface (instead of configured with the Anycast address). This verifies factors such as DNS, SecureSync being in sync, port 123 blocked of firewall, etc,
2. Verify either OSPF or BGP is truly Enabled and running (via the **Enable** checkbox being selected in the **Management -> NTP Setup** page, **NTP Anycast** button (left side of page). Then select either the associated **BGP**, **OSPF4** or **OSPF6** tab

### OSPF4



### BGP



3. (**BGP only**- not applicable to OSPF) in the **BGP** tab
  - A. Verify the values in the **AS Number** value and **Neighbor AS** fields is not the set to the same value. They must be two different unique numbers. Below is an example Journal entry showing both AS fields set to same value (65001)

[WEB] Enabled BGP (IPv4) Anycast: Address 100.100.100.100, Port eth2, AS Number 65001, Neighbor Address 46.235.32.1, Neighbor AS 65001 (spadmin)

#### 4. Get a **Save log bundle**

- Review the **Daemon** log for ospf/bgpd entries, to ensure one or the other is actually running (a couple examples below)

Feb 13 19:00:22 Spectracom /etc/init.d/zebra[12615]: WARNING: zebra has already been started

Feb 13 19:00:22 Spectracom /etc/init.d/bgpd[12619]: WARNING: bgpd is already starting

- Review the journal log to check the manual configurations of Anycast mode.

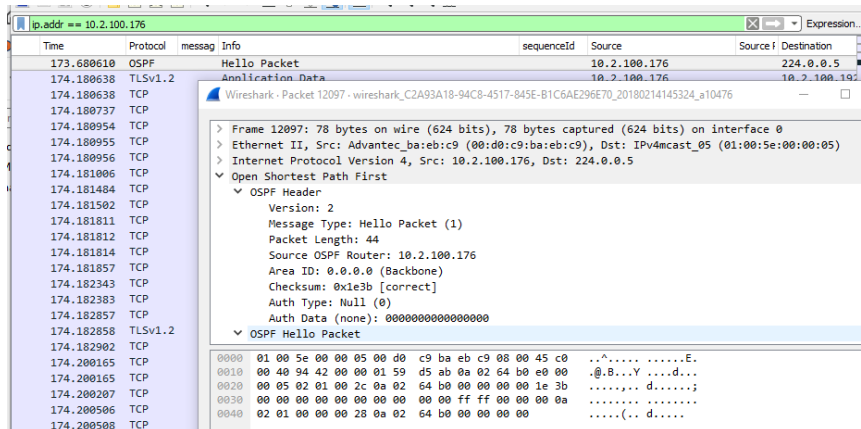
[WEB] Enabled BGP (IPv4) Anycast: Address 100.100.100.100, Port eth2, AS Number 65001, Neighbor Address 46.235.32.1, Neighbor AS 65001 (spadmin)

#### 5. Get a **Save Configs bundle** to review OSPF/Quagga configs

### External to the SecureSync

1. look at the the **Routing table** of the SecureSync's immediate **switch connected to the Anycast port** to see if the defined Anycast address is listed in this routing table. If NTP anycast is configured and RUNNING, it should be in this routing table. Its not added or is removed from the routing table if either BGP or OSPF is not Enabled or if there is a configuration issue with Anycast mode.
2. Verify the OSPF or BGP ports are open on the switch (**OSPF is on port 89** and BGP traffic is on **TCP port 179**)
3. Use **tcpdump** or get a **packet capture** to look for 'hello' messages (OSPF) being sent from the SecureSync to the switch every 10 seconds (see note above about network port numbers)

### OSPF Enabled



### BGP mode

- Per <https://networklessons.com/bgp/bgp-messages>, Apparently, the two BGP devices (SecureSync and Switch) first perform a tcp handshake before performing any BGP packet exchanges. So there wont be any "BGP protocol (tcp port 179) packets exchanged if the neighbor isn't really a bgp enabled switch.

### B) NTP over Anycast mode configs are not taking/being saved

- Verify the SecureSync is in sync (to an external reference or to itself) as required by this function. It has to first be synced before it can be configured.

---

## NTP Expert Mode

- Refer to the NTP expert mode tech note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast
- Required to use for NTP multicast mode
- Required to use with the NTP/External 1PPS input reference.
- Believe it can be used to provide NTP manycast mode

## NTP Setup page GUI fields not accessible while Expert mode is enabled

- Most NTP configurations in the **NTP Setup** page are not available while Expert mode is enabled. As of at least version 5.2.1:
  - **NTP autokey:** Not available while in Expert mode
  - **Symmetric key:** Can be used while in Expert mode (because ntp.keys is a different file than ntp.conf)

## ntp.conf file in expert mode

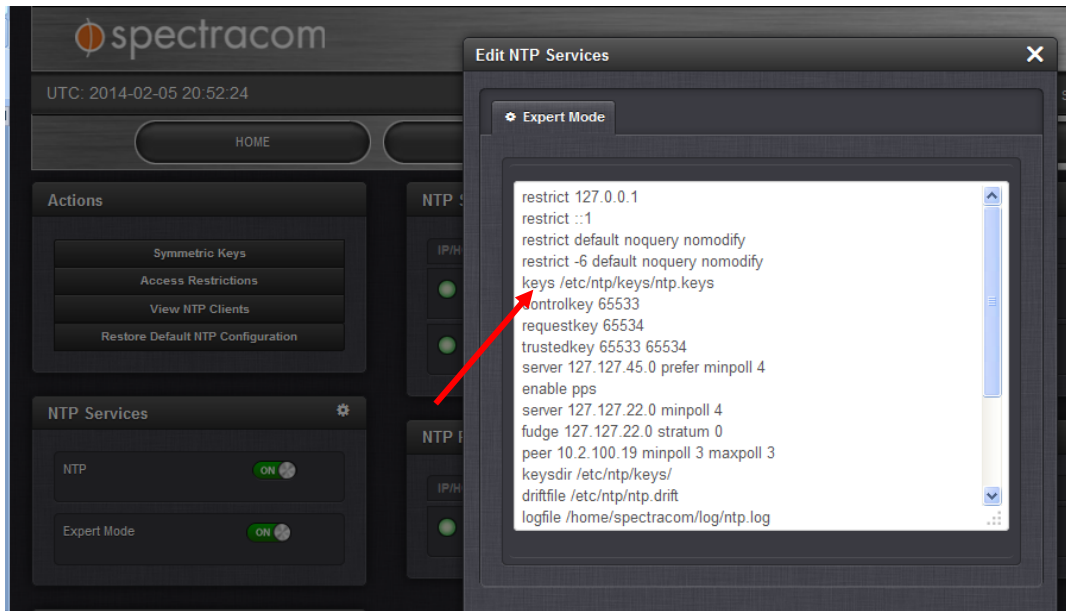
- Uses the same ntp.conf file in both modes
- spadmin account has rights to view (cat) the ntp.conf file via telnet connection, but not with ssh connection
- Even with Expert mode on, the ntp.conf file can only be edited via the web browser. This file can't be edited with an SSH connection (spadmin doesn't have write permissions for it, in the CLI interface).

## Enabling NTP Expert Mode

### A) New browser (Versions 5.1.2 and above)

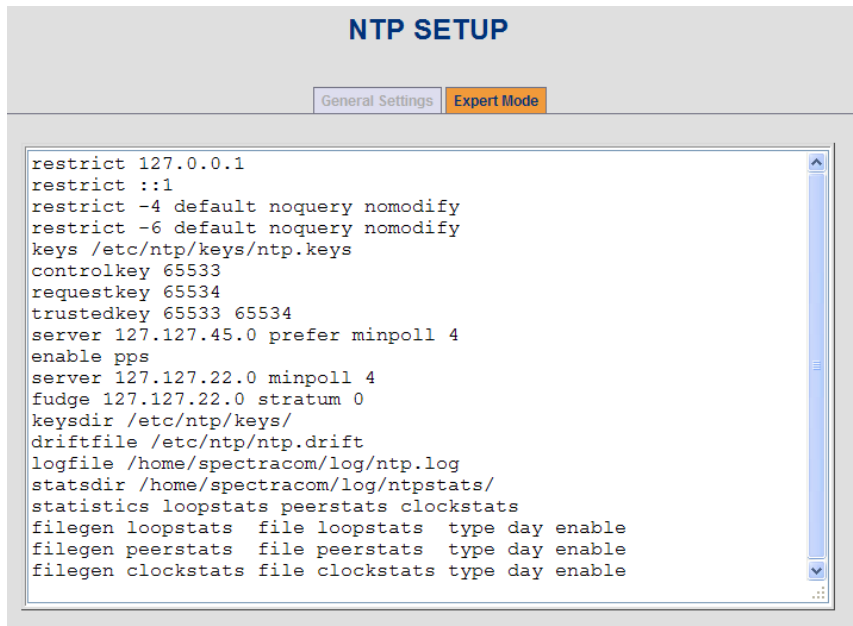
1. Go to the **Management** -> **NTP Setup** page of the browser
2. Enable NTP Expert Mode
3. Click on the gear next to "NTP Services" to open/edit the ntp.conf file
4. Leave Expert Mode enabled to retain settings
5. Disable Expert Mode to reset ntp.conf back to factory default settings





## B) Classic interface (Versions 5.0.2 and below)

1. Go to the **Network -> NTP Setup** page of the browser
2. Enable Expert Mode in the General Settings tab
3. Click on the Expert Mode tab to open/edit the ntp.conf file
4. Leave Expert Mode enabled to retain settings
5. Disable Expert Mode to reset the ntp.conf file back to factory default settings



---

## Operation as a Stratum 2 server (as of 10/20/09)

The current stratum-2 behavior will be as follows:

- The NTP running on the SecureSync will synchronize normally to the configured peers.
- Once a peer has been selected by NTP, KTS will be synchronized to that selected peer.
- When all peers are lost, the SecureSync will go into holdover and KTS will become the selected peer, synchronizing NTP using the undisciplined oscillator of the system

~~**Note:** The current design does not discipline the oscillator based on NTP, instead only steering the PPS based on NTP. That means the holdover characteristics of the unit in Stratum-2 will be based on the undisciplined oscillator of the unit.~~

**Update:** NTP can now discipline TCXOs and OCXOs, with host disciplining enabled.

---

## External 1PPS input to SecureSync

- For more information, refer to: 1PPS input (epp0)

**Note:** As also discussed in the NTP peering and External PPS input documents, we highly recommend listing more than one NTP server to sync with. Listing just one can cause NTP to continue to toggle between NTP input and Stratum 1 input, with periodic Holdover alarms asserted.

---

## Have a dedicated “Stratum 2” SecureSync report its actually “Stratum 1” instead

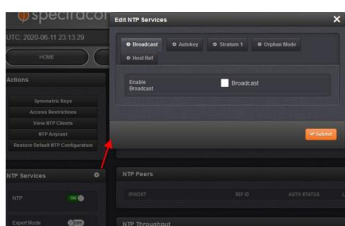
Per Keith after talking to Ron Dries (11 June 2020) Thanks for your follow-up status inquiry about desiring a SecureSync to sync via only NTP input (which would normally make it no higher than Stratum 2) while reporting to its clients that it's actually a “Stratum 1” server, instead.

I spoke to our Apps Engineering team this morning, and they were able to provide me with just one solution to do this. It's definitely a “non-standard” NTP configuration, with some draw-backs, if you would like to try it.

This unique configuration will be using only the dedicated NTP functionality inside the SecureSync (for instance, there will be no oscillator holdover capability if the NTP input is lost, the front panel time display/time reported in the web browser will not be the same as the time that NTP is providing to the network, the Sync status indications will be reporting the SecureSync is not in sync, etc). But NTP itself will be functional.

The one time we tried this abnormal configuration in the lab, it was observed that (as a direct result of timing jitter on the NTP input) NTP was periodically going out and back into sync, based on how well NTP was interpreting its time error levels. This will likely be observed by your SecureSync's down-stream NTP clients.

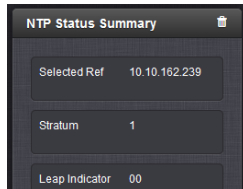
To configure this very unique “NTP Stratum 1” operation, with a Stratum 1 input, the NTP Expert mode is not needed. With Expert mode not enabled, navigate to the **Management** -> **NTP Setup** page of the browser. On the left side of this page, click the “gear” icon above the NTP service on/off slider switch (just to the right of “**NTP Services**”, as shown below). A popup window will open.



Select the “**Stratum 1**” tab, and three checkboxes will be displayed. Unselect the first two checkboxes, leaving only the last one selected. Press Submit, and the pop-up window will close.



The NTP Status summary table (bottom left corner of the same page) should then start to report that NTP is synced to the “upstream” NTP server’s IP address, while also reporting that its NTP is **Stratum 1** (as shown below):



Its now an NTP server, syncing only to one or more upstream NTP servers, and outputting to its NTP clients that it’s a Stratum 1 time server.

Please let me know how it works for your particular application. Thanks in advance!!

---

## NTP clockstats, loopstats and peerstats

Refer to (in “NTP for all products” towards the beginning of this document): [NTP ClockStats, Loopstats and Peerstats](#)

---

### \*NTP burst/iBurst mode

**Note (13 Feb 2013):** as of at least Archive software versions 4.8.8 and below, iBurst mode is not available via the web browser (a Mantis case is open requesting this capability). It is only available via the NTP Expert mode

**Update:** iBurst was added in version 5.0. NTP can now sync within just a couple of seconds of starting if NTP has a valid System Time reference (such as GPS or IRIG) to sync with.

---

## Issues related to NTP

### A) NTP reportedly not starting correctly (at least versions 5.1.4 and 5.1.7) LI (Leap indicator bits) set to 11 for extended duration

- Refer to Salesforce case 16920 and 19808
- Mantis case 2970: John Walters w/Raytheon has reported LI bits are periodically remaining set to “11” (3) for like 30 minutes after SecureSync goes into sync, preventing clients from being able to sync.
- This was observed in versions 5.1.4 and 5.1.7 (both were running NTP version 4.2.6p5).
- (9 Nov 15 KW) not sure what the resolution ended-up being (other than we are no longer running NTP v4.2.6p5)
  - Customer should update the software to the latest version of software.

---

## B) NTP logs not indicating all events (at least Archive versions 5.1.4 and 5.1.7)

- Mantis case 2969: NTP log no longer asserting certain log entries ("ntpd exiting on signal 15", "synchronized to PPS(0), stratum=0", etc)

---

## C) NTP not starting correctly (Archive versions 5.0.0, 5.0.1 and 5.0.2) LI bits remain 11 after NTP starts.

- Issue with archive versions 5.0.0, 5.0.1 and 5.0.2.
- LI bits (Leap indicator bits) are incorrectly set to "11" (3) preventing clients from being able to sync.
- NTP may remain Stratum 16
- Need to reboot or restart NTP (sometimes a couple of times)
- Fixed with version 5.1.2 update.

---

## D) NTP goes to and remains Stratum 16 after manually changing the time by more than one second (Archive versions 5.0.0, 5.0.1 and 5.0.2)

- Refer to Mantis case 2622
- If System Time is changed by more than one second with no references to correct the time (in Holdover) NTP will go out of sync and to Stratum 16 - and remain there indefinitely. It's not able to account for the manual time change.
- This will be fixed in version 5.1.2.

**Per Paul Myers** "NTP should restart if the KTS time and the Linux kernel time are more than 1 second different"

---

## E) NTP isn't remaining Stratum 1, as it should with a valid reference selected. Instead, it's going to Stratum 16 (Self reference not valid for NTP)NTP

- Refer to Salesforce case 16654 for Josh Foshee
- Refer to Mantis case 2954 (<http://cvsmantis.int.rolia.com/mantis/view.php?id=2954> )
- In software versions 5.2.0 and below, the Self reference - such as Self/EPP 0 (Local System/ External 1PPS input) is a valid reference for System synchronization. But this reference combination is not accepted by NTP as being a valid reference. So NTP can't sync to System Time. After a few moments. NTP switches from Stratum 1 to Stratum 16.

**Per Ron Dries, as reported in Mantis case 2954:** "When using a reference with self, i.e self/EPP0, the reference clock driver sees the self (local system) reference and sets the NTP stratum to 16. This should only occur for the hst1, stratum 2, operation. The Self reference should be valid if the system had a valid reference before switching to self."  
Temporary workaround is to change Self/EPP 0 to GPS/EPP0 which is valid for NTP.

**Note (29 Jan 15 KW):** "Local System" may also be the same situation. Mark Day had a customer using Local System/Freq 0. The SecureSync was in sync, but NTP remained S16.

## Notifications / Email alerts /SNMP

- Refer to the online SecureSync user [http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/Notifications.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/Notifications.htm)

### \*Notifications (SNMP traps and email alerts)/Alarms

#### Monitoring/Alert capabilities of installed Option Cards

**Note:** All of this info below is as of at least versions 5.5.1 (Feb 2017)

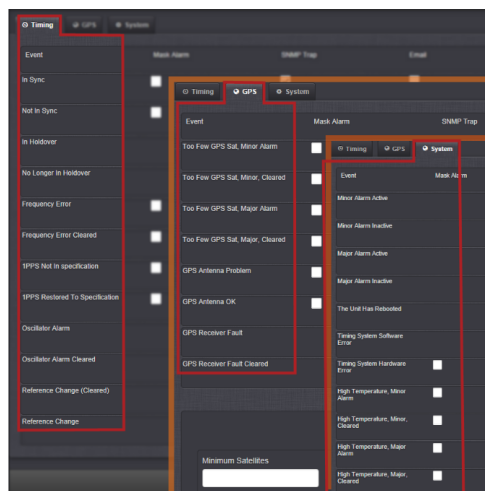
- No SNMP Traps/email alerts are directly available for Option Card functionality
- Only a couple of indirect (inherent) alarms/alerts are available for a loss of the currently selected input reference, if the selected input is being provided by an Option Card (such as IRIG, PTP, havequick inputs)
  - Loss of the selected input results in either “Reference Change” if there is another available reference which can be selected, or results in “Holdover” alert if there are no other references available for selection.

Q ...need to verify that the Spectracom Secure Sync.. can in fact fault detect and fault isolate to these optional cards? and where can I find the information WRT how the system can/will notify me of such a failure requiring maintenance..,

**A response from Keith (3 Feb 17)** Available SecureSync Option Cards which provide functionality for one or more outputs (such as the Model 1204-06 Gb Ethernet card, the IRIG outputs on the IRIG Option Cards, etc) and their associated output(s), are not monitored by the base SecureSync which the Option Cards are installed in. Therefore, there is no alert notification capability of the SecureSync itself, if there happens to be a problem with an output card or its particular output port. The alert would need to be provided by the other system which is connected to the SecureSync's output (an alarm/alert indicating the loss of its input signal for example).

SecureSync Option Cards which provide functionality for one or more inputs (such as the Model 1204-05 IRIG Input/Output Option Card for instance) or with each of its particular input(s), can result in indirect alerts/alarms being asserted- but only if this particular input is lost while it's the SecureSync's selected reference (alarms/alerts such as the “Reference Change” event is asserted if the SecureSync can switch to another available reference after its current reference is lost, or the Holdover alert is asserted if there are no other input references present/valid when this particular input signal is lost). Other than the alerts/alarms associated with the loss of the currently selected input reference signal, there is no continued monitoring of the Option Cards to detect if the Option Card or its particular input has a problem (the loss of a “not currently selected” input reference just results in that particular reference becoming “not valid” (unavailable for selection if the currently selected reference happens to become no longer present/becomes not valid) until the input has been restored. The loss of a “backup” reference is not an alarm/alert condition.

Note that with SNMP and/or Email alerts configured, the SecureSync can SNMP traps/email alert for many different conditions. All of these conditions (such as going into Holdover mode, loss of sync, etc), are shown in the **Management -> Notifications** page of the browser (via each of the three tabs at the top containing associated alerts. For your reference, Screenshots below are of the three tabs (note that each event can be individually configured to send an SNMP trap and, or an email alert but for simplicity, these screenshots are just omitting the email checkbox/email address field for each event).



## Configuration for Notifications (SNMP Traps and/or Emails) to be sent

- Refer to the online SecureSync user guide  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/CONFIG/Notifications.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/Notifications.htm)

## Inherent affects on the System when changes to Notifications are made (at least v5.9.2 and below)

- Refer to Salesforce cases such as 271831
- Refer to JIRA SSS-1114
- When any config changes are made to Notifications, statusd (status monitor daemon) will be restarted.
- statusd is what also monitors NTP Stratum and Sync state.
- While statusd is restarting, **NTP will inherently be reported as being Stratum 0, Not in sync**



- The **System** log will assert the following entry:

```
ERROR! Caught signal 6 (Aborted), address=00000000000bf0, pid=3056 (not reliable), tid=b73b76c0 (not reliable)
Backtrace: /lib/libEasyCpp.so(_ZN4Easy11crashActionEiPvS0_+0x1ad) [0xb7a18493]
/lib/libEasyCpp.so(_ZNK4Easy8FunctionlvNS_8TypeListIvS2_NS_9EmptyTypeES3_EEPvIS2_S2_EEclEIS2_S2_+0x24)
[0xb7a1a792] /lib/libEasyCpp.so(_ZNK4Easy6ActionlvNS_8TypeListIvS2_NS_9EmptyTypeES3_EEEclEIS2_S2_+0x38)
[0xb7a3c066] /lib/libEasyCpp.so(_ZN4Easy19signalActionWrapperEiP9siginfo_tPv+0x92) [0xb7a3b59a] /lib/libc.so.6(+0x32530)
[0xb742c530] /lib/ld-linux.so.2(+0x1092) [0xb7f3a092] /lib/libc.so.6(gsignal+0xe5) [0xb742c4b5] /lib/libc.so.6(abort+0x125)
[0xb741330a] /lib/libc.so.6(+0x79497) [0xb7473497] /lib/libc.so.6(+0x82538) [0xb747c538] /lib/libc.so.6(+0x84077)
[0xb747e077] /usr/lib/gcc/i686-pc-linux-gnu/9.3.0/libstdc++.so.6(_ZdlPv+0x1b) [0xb77a7b6b]
statusd(_ZN4Easy13checkedDeleteIN3Ntp7MonitorEEEvPT_+0x2e) [0x4c3c19]
statusd(_ZN5boost6detail18sp_counted_impl_pdIPN3Ntp7MonitorEPFvS4_EE7disposeEv+0x22) [0x4c5d84] stat (STATUSD)
```

**Per Tim Hammer (SSS-1114 16 Feb 2021)** I have confirmed this behavior on 5.8.9 (so it is not something introduced in the significant changes of 5.9.0, but I did not test to see how far back it exists).

The NTP status going to No Sync is “expected” behavior given that the implementation of the temperature monitoring & fan setting are in `daemons/statusd`, which is where NTP status monitoring is also done. When the fan settings are changed, `statusd` is restarted, so NTP status is temporarily unavailable.

(see `daemons/statusd/app/main.cpp::HandlerSIGHUP()` and `www2/app/Model/Tempd.php::createRecord()`)

However, I have been unable to find any obvious explanation for the error being logged. Based on the (partial) backtrace, the log message is coming from `EasyCPP/CrashHandler.cpp:crashAction()`. This cannot be coming from the `SigHUP` request.

The “beginning” of the stack trace (as far as we can see in the log) indicates it might be in `easycpp/include/EasyCpp/DeleteHelpers.h::checkedDelete()` where it could be trying to delete an invalid pointer?

```
template<class T> void checkedDelete(T *ptr)
{
 typedef char TypeMustBeComplete[sizeof(T) ? 1: -1];
 (void)sizeof(TypeMustBeComplete);
 delete ptr;
}
```

However, determining how it gets here will require more action to identify the rest of the stack.

## Web browser config

### A) New browser: *Management* -> *Notifications* page (Timing tab, GPS tab, and System tab at the top)

- The three tabs at the top of the page- *Timing*, *GPS* and *System*- contain the associated Notifications (these are the only notifications available to be sent from the NTP server)

The screenshot shows the 'Events' configuration page with the 'Timing' tab selected. The page contains a table with columns for 'Event', 'Mask Alarm', 'SNMP Trap', 'Email', and 'Email Address'. The following table represents the data shown in the screenshot:

| Event                 | Mask Alarm               | SNMP Trap                           | Email                    | Email Address        |
|-----------------------|--------------------------|-------------------------------------|--------------------------|----------------------|
| In Sync               | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Not In Sync           | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| In Holdover           | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| No Longer In Holdover | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Frequency Error       | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |

### Three tabs (screenshots shown with 5.8.9 installed)

#### A) **TIMING** Tab

The screenshot shows the 'Events' configuration page with the 'Timing' tab selected. The page contains a table with columns for 'Event', 'Mask Alarm', 'SNMP Trap', 'Email', and 'Email Address'. The following table represents the data shown in the screenshot:

| Event                          | Mask Alarm               | SNMP Trap                           | Email                    | Email Address        |
|--------------------------------|--------------------------|-------------------------------------|--------------------------|----------------------|
| In Sync                        | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Not In Sync                    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| In Holdover                    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| No Longer In Holdover          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Frequency Error                | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Frequency Error Cleared        | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| 1PPS Not In specification      | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| 1PPS Restored To Specification | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Oscillator Alarm               | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Oscillator Alarm Cleared       | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Reference Change (Cleared)     | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| Reference Change               | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |

## B) GPS Tab

| Event                           | Mask Alarm               | SNMP Trap                           | Email                    | Email Address        |
|---------------------------------|--------------------------|-------------------------------------|--------------------------|----------------------|
| Too Few GPS Sat, Minor Alarm    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Too Few GPS Sat, Minor, Cleared | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Too Few GPS Sat, Major Alarm    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Too Few GPS Sat, Major, Cleared | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| GPS Antenna Problem             | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| GPS Antenna OK                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| GPS Receiver Fault              | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| GPS Receiver Fault Cleared      | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |

Minor Alarm Threshold

Minimum Satellites:  Duration Below Threshold (s):

Major Alarm Threshold

Minimum Satellites:  Duration Below Threshold (s):

### Opt-IDM: available Broadshield notifications (v5.7.1 and above only, and only with Opt-IDM enabled)

- Enabled or masked in the **Management** -> **Notifications** page of the browser, **GPS** tab (only displayed if "IDM Suite" is enabled)
- Only two notifications available for Broadshield (as of at least 5.8.9)
- These two notifications are only displayed/available in versions 5.7.1 and above, and only when Opt-BSH: BroadShield is installed/enabled
- email alerts only (no SNMP traps available) as of at least update v5.8.9

| Event                                | Mask Alarm                          | SNMP Trap                           | Email                    | Email Address        |
|--------------------------------------|-------------------------------------|-------------------------------------|--------------------------|----------------------|
| Too Few GPS Sat, Minor Alarm         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Too Few GPS Sat, Minor, Cleared      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Too Few GPS Sat, Major Alarm         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Too Few GPS Sat, Major, Cleared      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| GPS Antenna Problem                  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| GPS Antenna OK                       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| GPS Receiver Fault                   | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| GPS Receiver Fault Cleared           | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| BroadShield Critical, Major Alarm    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| BroadShield Critical, Major, Cleared | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |

**Notice: No SNMP Trap Checkboxes, just Email alerts (at least update v5.8.9 and below)**



## C) SYSTEM Tab

| Event                            | Mask Alarm                          | DSNP Trap                           | Email                    | Email Address        |
|----------------------------------|-------------------------------------|-------------------------------------|--------------------------|----------------------|
| Minor Alarm Active               | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Minor Alarm Inactive             | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Major Alarm Active               | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Major Alarm Inactive             | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| The Unit Has Rebooted            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| Timing System Software Error     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| Timing System Hardware Error     | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| High Temperature, Minor Alarm    | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| High Temperature, Minor, Cleared | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| High Temperature, Major Alarm    | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |
| High Temperature, Major, Cleared | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="text"/> |

Minor Alarm Threshold

Minimum CPU Temperature (C):

Readings Above Threshold:

Major Alarm Threshold

Minimum CPU Temperature (C):

Readings Above Threshold:

**Note (at least 5.8.9 and below):** Notice there are no “Mask Alarm” checkboxes available from Major Alarm/Minor Alarm and Reboot (these alerts cant be masked)

**Note:** These Mask Alarms settings are stored in the **home\spectracom\config\notcf.conf** file (as shown below):

```

D:\Spectracom\customer logs\Spectracom\configs from 5.8.0\securesync\home\spectracom\config\notcf.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
notcf.conf [3]
1 1 0 1 0
2 2 0 1 0
3 3 0 4 0
4 3 0 1 0
5 4 0 4 0
6 4 0 1 0
7 5 0 1 0
8 6 0 1 0
9 9 0 1 0
10 10 0 1 0
11 11 0 1 0
12 12 0 1 0
13 13 0 1 0
14 14 0 1 0
15 15 0 1 0
16 16 0 1 0
17 23 0 1 0
18 24 0 1 0
19 25 0 1 0
20 26 0 1 0
21 27 0 1 0
22 28 0 1 0
23 35 0 1 0
24 36 0 1 0
25 38 0 1 0
26 53 0 4 0
27 54 0 4 0
28 55 0 4 0
29 56 0 4 0
30 46 0 3 0
31 46 0 3 1
32

```

## B) Classic interface browser: *Tools* -> *Notification* page

| Event                          | Mask Alarm               | SMPP Trip                           | Email                               | Email Address                         |
|--------------------------------|--------------------------|-------------------------------------|-------------------------------------|---------------------------------------|
| In Sync                        | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | morgan.randolph@spectracom.orolia.com |
| Not In Sync                    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | morgan.randolph@spectracom.orolia.com |
| In Holdover                    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | morgan.randolph@spectracom.orolia.com |
| No Longer In Holdover          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | morgan.randolph@spectracom.orolia.com |
| Frequency Error                | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                       |
| Frequency Error Cleared        | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                       |
| 1PPS Not In specification      | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                       |
| 1PPS Restored To Specification | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                       |
| Reference Change               | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                       |
| Reference Change (Cleared)     | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            |                                       |
| Oscillator Alarm               | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                       |
| Oscillator Alarm Cleared       | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                                       |

### Issues associated with “Notifications”

1. **Customer report (v5.8.6) changes to the Mask Alarm checkboxes are not being retained (such as when navigating from one of the three “grouping” tabs to another tab)**
  - Refer to Salesforce Cases 217448/217670
  - I have not been able to duplicate this. I changed tabs without pressing Submit and changes persisted (but still need to press the Submit button before changing to a different page of the browser).
  - Update: Customer was not pressing the **Submit button**. The Submit button is “hidden” on this page, as you need to scroll down first, before seeing it. So it can be easy to forget to push Submit before switching between the three tabs (or switching to another page of the browser).

---

## **\*\*Nullmailer/Email Alerts**

### **A) 1.4.2 Nullmailer:**

From [http://wiki.linuxquestions.org/wiki/Nullmailer#Running\\_the\\_daemon](http://wiki.linuxquestions.org/wiki/Nullmailer#Running_the_daemon): "nullmailer is a simple and secure relay-only mail transport agent

- Nullmailer is an email package automatically included in Gentoo (versions 5.0.0 and above)
- We don't configure or use Nullmailer
- Because we don't configure/user nullmailer, but it's still running, we noticed in version 5.0.2 that it was creating files for all the events that weren't being sent. Issue fixed in 5.1.2.

Refer to the **rex.d.log** for Nullmailer log entries: [rex.d.log \(daemon log\)](#) and [rex.d.bone log](#) Note that the rex.bone log MOTD time stamp gets updates each time Nullmailer runs.

### **B) Email Alerts**

- For more information on Email alerts refer to: [!:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP](#)
- We use the 3rd party application called "Nail" for linux (now called mailx) to send emails.
- Refer to sites such as <http://en.wikipedia.org/wiki/Mailx> and <http://www.computerhope.com/unix/umailx.htm> for more info on mailx

## **Configure Email/SMTP setting**

Refer to the Email tech note that Morgan created:

- At: [\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP](#)
- On our website at: <http://spectracom.com/sites/default/files/document-files/Email%20Notification%20Setup%20SecureSync%20and%20NetClock.pdf>

## **Desire to send alerts to more than email address**

- Limited to just one "To" email "address per each notification (limitation of mailx). But it can be configured to send to multiple "Cc" addresses (comma separator with no spaces before or after the comma)
- With the earlier Nail (can't list more than one recipient per event). I recall this being a limitation of Nail (11 Apr 2013)
- However, can configure each to be sent to more than one "Cc" address – by using a 'comma' separator (with no spaces before or after the comma in the SMTP settings (see below )

**Email from Ron Dries (25 Jun 16)** I just tried adding set autocc to the email configuration file and it worked. The syntax was as described in that document.

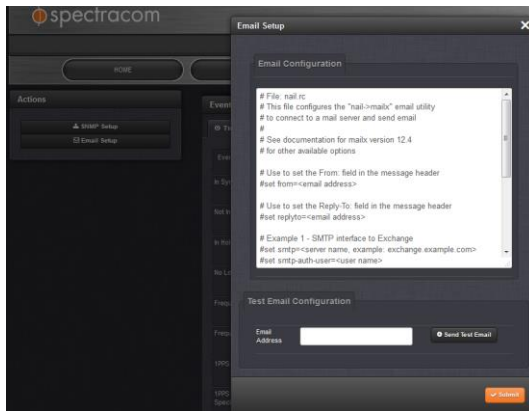
Set autocc=<email address 1>,<email address2>,...

I sent a test email to myself and you and I saw your email address on the CC line when I received the test email.

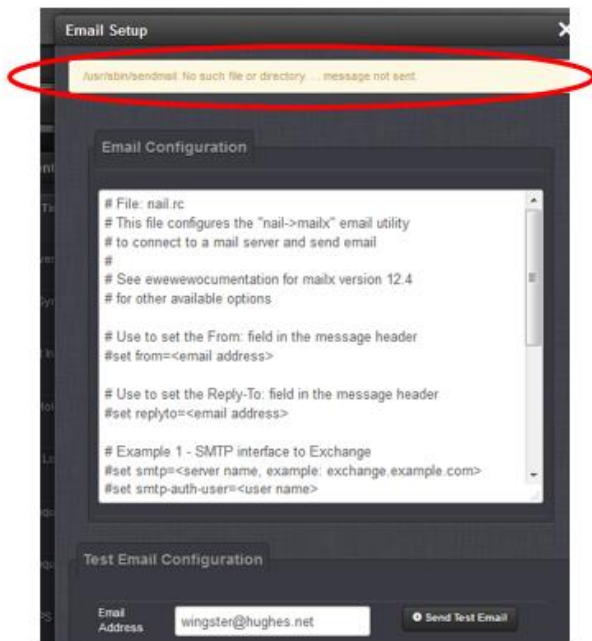
### **C) Newer web browser (v5.1.2 and above)**

**Management** -> **Notifications** page of browser

- Press the "Email Setup" on the left side of the page.



**Error message “ /usr/sbin/sendmail: No such file or directory...message not sent.” is displayed when pressing the “Send Test Email” button, while editing the configs (and before pressing Submit:**



- If the “Send Test Email” button is pressed while making any changes to the email configs, and before the Submit button is pressed to save the changes just made, this error will be displayed when pressing the Test button before hitting the Submit button
- To prevent this condition, press the “Submit” button after making any changes to the configs, and before pressing the “Send Test Email” button.

**Email Keith sent (21 Jun 17)** We wanted to let you know we were able to duplicate the error message you observed, which allowed us to determine what causes it to be displayed.

This is actually a very minor condition which occurs if you make any changes to the email configuration, **and then press the “Send Test Email” button, before pressing the “Submit” button in the same window.** The “Send Test Email” button doesn’t save the changes that are “in process”. So the Submit button needs to be pressed first, before trying to send a test email. The Submit button will close the window and the “Send Test Email” button can be pressed after re-opening the same window.

After editing the email config file as necessary, please press **Submit**. Then after reopening the “**Email Setup**” window, now press the “Send Test Email” button. The “sendmail” message you were seeing previously should no longer be displayed at the top of the window.

We would like to know if there is any other message being displayed after pressing the test button.

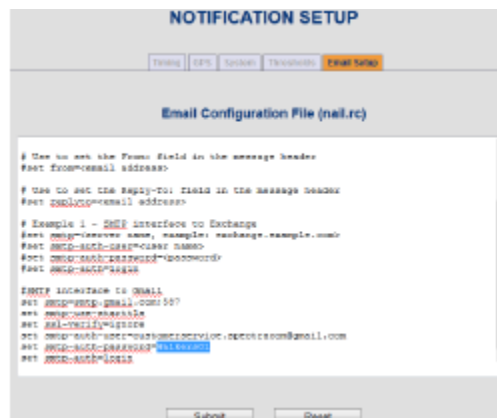
## 1. Example smtp setup for Outlook 365 SMTP from a workstation that worked for Keith

**Note:** Outlook 365 doesn't need to be open to send an email using it

```
Example 1 - SMTP interface to Exchange87
set smtp=smtp.office365.com:587
set smtp-use-starttls
set ssl-verify=ignore
set smtp-auth-user=keith.wing@spectracom.rolia.com
set smtp-auth-password= (email still sent with no password)
set smtp-auth=login
set from=keith.wing@spectracom.rolia.com
```

**Test Email Configuration** -> "Email address" field: [keith.wing@spectracom.rolia.com](mailto:keith.wing@spectracom.rolia.com) or [techsupport@spectracom.rolia.com](mailto:techsupport@spectracom.rolia.com)

## 2. Example Gmail SMTP setup that worked using the classis interface (performed by Sam Otto)



### Example smtp setup for Exchange server

➤ Enter just one email address for each notification type to be sent to, as desired

Q. According to User Manual, it seems that we can use "Microsoft Exchange" and "Gmail" as SMTP server which we can send Email to. Can we set SMTP server other than "Microsoft Exchange" and "Gmail" in "Email setup" tab of "NOTIFICATION Setup" page?

**A. Reply from Dave Lorah:** The email alerts function can use any exchange server to send emails, not just MS and Gmail only.

**Email to Bruce Carey 10/10/11 based on feedback from Mike Sander:**

Regarding the SecureSync email alerts functionality, I have some feedback for you, from our Engineering team:

### Other Notes

- 1) In SecureSync, we enter the short form of the user name, in your particular case, "Careyb"
- 2) The settings for exchange servers are tricky and in our particular case, required some back and forth with our IT group to allow it to start working.
- 3) The SecureSync uses a linux-based email utility called "nail" to send email alerts. The **Notifications->Email Setup** window is editing the standard "nail.rc" configuration file in the background. So you can look at documentation for "nail.rc" for advanced information about configuring email notifications (refer to sites such as

<http://linux.die.net/man/1/nail> for example).

- 4) You can also invoke “nail” for a command line using either telnet (in a command prompt window, type telnet xxx.xxx.xxx.xxx - where x is the IP address of the NTP server) or the front panel serial port (connecting a PC running HyperTerminal to this port using a straight-thru serial cable- pinned 2 to 2, 3 to 3 and 5 to 5 for a minimum pinned cable). Refer to the attached Application Note regarding HyperTerminal.

Here’s an example:

```
>nail -s "test" user@XYZ.com
```

```
Testing testing testing
```

```
<ctrl-d>
```

Nail may display a useful error.

- 5) You should try commenting out the “gmail configuration” and just exposing the exchange configuration. The emails can’t be sent using two servers and will use the last definition in the file.

#### Example Gmail SMTP setup that worked (performed by Sam Otto)

```
NOTIFICATION SETUP
Timing GPS System Thresholds Email Setup
Email Configuration File (nail.rc)
Use to set the From: field in the message header
#set from=<email address>
Use to set the Reply-To: field in the message header
#set replyto=<email address>
Example 1 - SMTP interface to Exchange
#set smtp=<server name, example: exchange.example.com>
#set smtp_auth_user=<user name>
#set smtp_auth_password=<password>
#set smtp_auth_login
#SMTP interface to Gmail
set smtp=smtp.gmail.com:587
set smtp-use-ssl=0
set ssl-verify=ignore
set smtp_auth_user=customerservice.spectracom@gmail.com
set smtp_auth_password=No!ker@1
set smtp_auth_login
Submit Reset
```

#### “Root@xxxx” domain name sent in the email alerts

**Note:** Refer to Mantis case 1742/Salesforce case 6030 for TOYO.

- By factory default, Emails that are sent indicate “root@spectracom” even though the domain name for the network port is configured as a different value (always “root@” followed by the domain name).

#### Update to the “Note” below about “root”

Dave Sohn has found that NAIL has the ability to edit this name, without needing to update to a newer version of software. Version 4.8.7 will add the information below to the examples, so customers can see how to edit the “From” and “Reply-To” names.

The desired change can be made in the **Tools -> Notifications** page of the web browser, “**Email Setup**” tab, as shown below:

Below are the commented option lines that can be used to set the **From:** and **Reply-To:** fields in the email notifications sent from the SecureSync. Just add the “set” line into the existing email configuration file using the Web browser and then press Submit”

```
Use to set the From: field in the message header
```

```
#set from=<email address>
```

# Use to set the Reply-To: field in the message header  
#set replyto=<email address>

**Note:** (8-23-12 KW- This “Note” has been superseded by the “Note” above –no need to perform software update) In at least versions 4.8.6 and below, the domain name (sent in the email alert) after the “@” sign can be configured via the web browser. However this email value will always begin as “root@” (there is currently no way to change “root” to another value. For example, “**root@spectracom**”. Refer to Mantis Case 1742/Salesforce 6030 (TOYO) for more information,

**Q.** Although "Domain setup" field was set as "domain202",SecureSync sent E-mail to SMTP server by using "root@Spectracom" domain. Why does SecureSync send E-mail to SMTP server by using "root@Spectracom" domain?

**A. (reply from Keith to Masataka, after talking to Mark Goodlein)**

The emails that are sent reference the DNS Host name for the SecureSync box. It does not use the domain name fields for each of the network ports.

The host name for the SecureSync is configured in the “**Hostname**” field which is located in the **Network -> General Setup** page of the browser, “**General**” tab.

---

## \*\*SNMP (SNMPv1/SNMPv2C/SNMPv3)

### SNMP package in SecureSync

- 1200/2400 SecureSync uses the open source SNMP package called Net-SNMP (NetSNMP)
  - From/supported by: **Sourceforge** <https://sourceforge.net/>
- For details on Net-SNMP, refer to **the Net-SNMP WIKI**: <http://www.net-snmp.org/wiki/index.php/> and <http://www.net-snmp.org/docs/FAQ.html>
- For more information on SNMP refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP>

---

### NET-SNMP version

- SNMP software version changes- refer to:<http://www.net-snmp.org/about/ChangeLog.html>
- CLI command to read NET-SNMP version is: **version snmp** <enter>
- NET-SNMP version is also reported in the SNMPd.log file at each boot up

### Software changes associated with Net-SNMP (ascending order)

SecureSync System Version	Corresponding Net-SNMP Version	Notes
<a href="#">Versions 5.1.7 and below</a>	5.6.1	
<b>Versions 5.2.0 (Feb 2015) and above</b>	5.6.2.1	In order to update SNMP to the newer version, our snmpsad subagent needed to also be updated.
<b>Version 5.2.1</b>	X (no change- still 5.6.2.1)	Added a patch to Net-SNMP to address SNMPD crashing. This patch didn't change the Net-SNMP version.
<b>Version 5.8.4</b>	X (no change- still 5.6.2.1)	
<b>Version 5.8.5 (July 2019)</b>	X (no change- still 5.6.2.1, as of at least v5.9.2)	<b>Per 5.8.5 release notes</b> : "Corrected behavior of SNMP in order to retain engine IDs on each startup."

---

### SNMP MIB files/Object IDs

- **Path to the MIB files stored in the Model 9400 series**: Home/Spectracom/mibs
  - The SNMP object numbers of ".1.3.6.1.4.1.18837." are for the Spectracom-specific objects.
  - The SNMP object numbers of ".1.3.6.1.4.1.8072." are objects associated with Net-SNMP.
  - The SNMP object numbers of ".1.3.6.1.4.1.2.1" are objects associated with RFC-1213.

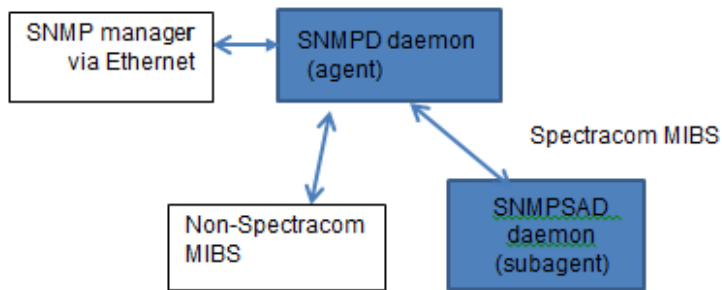
---

### SNMPD and SNMPSAD daemons

- There are three daemons that run for SNMP:
  - **SNMPD**: the agent running in the Linux OS
  - **SNMPSAD**: the subagent running in Spectracom application
  - **SNMPSAL**: our daemon that restarts SNMPSAD if it crashes



## SNMP Basic block diagram



**(Modified) email from Mark Goodlein to Morgan Stanley (7/1/12)**

For SNMP:

There are 2 daemons that run, one is the agent (SNMPD) which handles snmp protocol and some published system mibs. The other is a subagent (SNMPSAD) which connects to the agent and handles the Spectracom-specific mibs.

---

## \*\*Remote Monitoring / SNMP configuration

### Enterprise-level network monitoring tools

- Refer to the "...network monitoring tools" section of the Custserviceassistance document

---

## SNMPd config file

- Path to the snmpd.conf file in the time server: home/spectracom/config
- Refer to: <http://www.net-snmp.org/docs/man/snmpd.conf.html> and
- <http://www.net-snmp.org/wiki/index.php/Vacm> (VACM info)

**snmpd** supports the View-Based Access Control Model (VACM) as defined in RFC 2575, to control who can retrieve or update information. To this end, it recognizes various directives relating to access control.

## SNMP configuration

- Refer to the **SecureSync SNMP Tech Note**: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP>
  - Newer web browser: *Management* -> *SNMP Setup* page
  - Classic interface browser: *Network* -> *SNMP Setup* page

"Restore Default SNMP Configuration" button (newer web browser only)

**Note:** this function is not available in classic interface web browser



- The newer black/charcoal browser now has a “Restore Default SNMP Configuration” button in the Management -> SNMP Setup page which resets just the SNMP configs (alleviating the need to perform a full clean of all configs). Not sure what rev (either version 5.1.7 or before) this button was added to the newer browser.
- Brian Carlson with Harris was seeing weird issues with the configuration of the Notifications page and traps not being sent when they should. Using this button and reconfiguring SNMP fixed these peculiar issues.

## A) SNMP User configuration (SNMP gets and sets)

### 1. SNMP V1/V2c user configuration

- **Unsecure:** Unlike SNMPv3, v1 and v2c do not use either encryption or authentication.

Configuration using newer black/charcoal browser (versions 5.1.2 and above).

**IP address field:** If it is set to a specific IP it will only respond to that IP address, if it is set to a subnet it will only respond to that subnet. Leave field blank and Submit- Sets it to “default” to allow any user (from any IP address) to query the SecureSync.

### SNMP Community/Username field

- **Versions 5.2.1 and above:** Can be **1 to 31** characters (refer to Mantis case 2923).
- **Versions 5.2.0 and below:** Can be **8 to 32** characters (earlier rev SecureSync Manual incorrectly stated “between 4 and 32 characters in length.”)

### Classic interface browser:

SNMP Community/Username field

### 2. SNMPv3 user configuration

Newer web browser

### SNMPv3 User name (username) field

(In at least update versions 5.7.1 through 5.9.2 and below) Enter **the 8 to 32-character** user (principal) on whose behalf the message is being exchanged

- Per Salesforce Case 261971, this min requirement of at least eight (8) characters appears to be a browser issue (not a Net-SNMP requirement)
- Refer to JIRA Ticket SSS-536 for request to lower the requirement to 1 to 32 characters (Per this JIRA ticket, it used to be 1 to 32 characters, before version 5.7.1/5.8.1 were released)

**Per Ron Dries (13 Apr 2021)** There is a JIRA ticket already to fix the validation to allow a SNMP username to be 1-32 characters. That JIRA is SSS-536.

**Status Update:** JIRA SSS-536 was fixed in update version 5.9.3 (Nov 2021). Should now be back to being able to be 1 to 31 characters in length

### SNMPv3 Priv Passphrase field

Enter an **8-32 character** passphrase for encryption

- Per case 261971 this requirement appears to be a Net-SNMP requirement (not just a browser requirement)

➤ **Per:** <http://net-snmp.sourceforge.net/docs/README.snmpv3.html>

*WARNING: SNMPv3 pass phrases must be at least 8 characters long!*

### (Applicable to versions 5.9.0 and above) Auth/No Priv selection

#### Software versions 5.9.0 and above

- Per v5.9.0 Release Notes “Added a No Privacy option to SNMPv3 settings”

Previously, only Auth/Priv supported

## SNMP trap configuration/operation

- Refer to SecureSync online user guide:  
[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/SNMP\\_Traps.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Traps.htm)
- Refer to the SecureSync SNMP Tech Note: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP>

### A) SNMPV3 traps (note the SecureSync sends “traps” - not “informs”)

- Refer to: <http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html>



VERSION	COMMUNITY	DESTINATION IP	PORT	ENGINE ID	AUTH TYPE	PRIV TYPE
v3	example3	10.10.128.1	162	0x1234	MD5	AES

### Software versions 5.9.0 and above

- Per v5.9.0 Release Notes “Added a No Privacy option to SNMPv3 settings”

### SNMP user section of the browser

- The SNMPv3 user section of the SecureSync does not need to be created in order to send a trap that Wireshark can see (just filling in the V3trap section will allow a trap to be sent). But if the SNMPv3 user section isn't created, the SNMP manager won't be able to successfully authenticate/decrypt the traps that it received (the traps will be displayed in Wireshark but not in the manager).

### SNMP Community/User field

- **Versions 5.3.0 and above:** Can be 1 to 31 characters (refer to Mantis case 3103).  
Note this change was supposed to be in the version 5.2.1 update, but it wasn't included.
- **Versions 5.2.1 and below:** Can be 8 to 32 characters (SecureSync Manual incorrectly stated “between 4 and 32 characters in length”).

### EngineID (Engine ID) field for SNMPv3 traps

- Refer also to: <http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html> for info on “Traps” versus “Informs” (SecureSync sends “Traps”- not “Informs”)., Scroll down to “**SNMPv3 TRAPS**”
  - **For SNMP Gets/Sets:** The SNMP Manager sends its EngineID to the SecureSync. There is no need to define an EngineID in the SecureSync for gets/sets
  - For **SNMP traps:** The EngineID field needs to contain an EngineID value in order to send any traps. Apparently, depending on what SNMP Manager is being used, this field may need to be populated with the SecureSync's EngineID- not the EngineID of the SNMP manager.

**Note:** refer to JIRA ticket SSS-449 <https://spectracom.atlassian.net/projects/SSS/issues/SSS-449?filter=addedrecently> for more details

In at least software versions 5.7.1 and below, the SecureSync's EngineID is not displayed anywhere in the browser, and is not available via a supported CLI call either (the JIRA case above is recommending it be reported in the browser for convenience to the customer)

Currently, the customer must read our engineID from MIB using and SNMPGET (which is inconvenient)

An **SNMP WALK OR GET** can read the OID (part of the SNMP-Framework-Mib file, which can be downloaded at the link) **.1.3.6.1.6.3.10.2.1.1** (which returns the EngineID of the SecureSync), refer to <http://www.net-snmp.org/docs/mibs/snmpFrameworkMIB.html>

## B) Using an SNMPv2c Get to obtain the SecureSync's SNMPv3 EngineID value:

- 1) Configure an SNMPv2c user (if one has not yet been added to the SEcureSync)
- 2) open a telnet or SSH session to the SecureSync

Type the following command **snmpget -v 2c -c snmptest xxx.xxx.xxx.xxx**

**.1.3.6.1.6.3.10.2.1.1.0**<enter> (where "zzzzz" is the community name of the V2c user and where "xxx.xxx.xxx.xxx" is the IP address of the SecureSync).

See the example response below (note the string **value** will vary):

```
spadmin@Spectracom ~ $ snmpget -v 2c -c snmptest 10.2.192.226 .1.3.6.1.6.3.10.2.1.1.0
SNMP-FRAMEWORK-MIB::snmpEngineID.0 = Hex-STRING: 80 00 1F 88 80 9A 9B 94 3D 89 EC C4 5A
spadmin@Spectracom ~ $
```

- 3) In the "EngineID" field of the SecureSync, first type the two-character (one number and one letter) value of: **0x** (the number "0" and not the letter "O") followed by the values in the hex-String response (with no spaces between "0x" and the string values, and remove all the spaces between each set of the two character values in the response.

**Example value to enter into the "EngineID" field based on the example response string above:**  
**"0x80001F88809A9B943D89ECC5A"**

**snmpget -v 2c -c snmptest 10.10.163.202 .1.3.6.1.6.3.10.2.1.1.0**

## C) Obtaining SecureSync's EngineID via an SNMP Manager program

(need to first download and install the **SNMP-Framework-MIB** file from the Internet: <http://www.net-snmp.org/docs/mibs/snmpFrameworkMIB.html>)

The screenshot displays an SNMP Manager interface. On the left, a tree view shows the hierarchy of MIB objects, with 'snmpEngineID.0' selected under 'snmpFrameworkMIBObjects'. The main area shows a table of object values, including #OutNcastPkts, #OutDiscards, #OutErrors, #OutOl.en, and #Specific. The bottom pane shows the object's description and syntax.

Object ID	Value
#OutNcastPkts.6	0
#OutNcastPkts.7	0
#OutNcastPkts.8	0
#OutDiscards.1	0
#OutDiscards.2	0
#OutDiscards.3	0
#OutDiscards.4	0
#OutDiscards.5	0
#OutDiscards.6	0
#OutDiscards.7	0
#OutDiscards.8	0
#OutErrors.1	0
#OutErrors.2	0
#OutErrors.3	0
#OutErrors.4	0
#OutErrors.5	0
#OutErrors.6	0
#OutErrors.7	0
#OutErrors.8	0
#OutOl.en.1	0
#OutOl.en.2	0
#OutOl.en.3	0
#OutOl.en.4	0
#OutOl.en.5	0
#OutOl.en.6	0
#OutOl.en.7	0
#OutOl.en.8	0
#Specific.1	0.0
#Specific.2	0.0
#Specific.3	0.0
#Specific.4	0.0
#Specific.5	0.0
#Specific.6	0.0
#Specific.7	0.0
#Specific.8	0.0

Loading MIBs C:\Temp\SNMP-FRAMEWORK-MIB.bt  
MIB(s) Loaded Successfully.  
Sent GET request to 10.2.192.226: 161  
snmpEngineID.0 80 00 1F 88 80 9A 9B 94 3D 89 ec c4 5a

Description: **snmpEngineID**  
Syntax: SnmpEngineID  
Access: read-only  
Index: Reference  
Object ID: .1.3.6.1.6.3.10.2.1.1  
Description: "An SNMP engine's administratively-unique identifier. This information SHOULD be stored in non-volatile storage so that..."

- 1) Take the returned value,
  - 2) Add "0x" to the front of this value and remove all the spaces between each two character value
  - 3) Place this full value (with no spaces) in the SecureSync's SNMPv3 EngineID field
- SNMPv3 traps will only be sent from the SecureSync if an EngineID (beginning with "0x") field has been populated when configuring v3 traps in the SecureSync. Without a valid engineID (which is then pasted into the V3 trap section of the SecureSync) no v3 traps are sent.
  - in at least v5.7.1 and below, the SecureSync enforces Auth, Priv in SNMPv3 (can't configure no auth,no priv).
  - The Manager sends a message to the SecureSync when it's being setup for SNMPv3 users in order to generate the contextID/engineID.

No.	Time	PTP_L1_61	Protocol	Peer Clock Stratum	VLAN	Info
531	21:00:28.25810000		SNMP			encryptedPDU: privkey unknown
2716	21:01:58.18720500		SNMP			get-request
2717	21:01:58.18783000		SNMP			report 1.3.6.1.6.3.15.1.1.4.0
2718	21:01:58.21694700		SNMP			get-request
2719	21:01:58.21764400		SNMP			report 1.3.6.1.6.3.15.1.1.2.0

- The engineID can't just be an "arbitrary" value such as "0x1a" for example.

#### D) Newer black/charcoal web browser (v5.1.2 and above)

Management -> SNMP Setup page of the browser:



**Note:** The following configurations in this particular section are only needed when sending SNMPv3 Traps to the time server (they aren't required when using SNMPv1/SNMPv2c).

**Engine ID (SNMPv3):** Enter the SNMP EngineID of the authoritative SNMP engine involved in the exchange of this message.

**Note:** The Engine ID is a 12 octet, hexadecimal value that needs to be externally created by a user and then entered into the SecureSync's web browser. This value needs to begin with a "0x". If this field is left blank, its defaults to "0x01". If your SNMP Manager/MIB browser generates a hex "Content ID" value, this value can be used as the Engine ID.

Q There appears to be nothing in the GUI to lock down the engine id.

**A reply from Oleg (11 Apr 17)** Correct. The engineID on SecureSync is determined automatically, using two reasonably non-predictable values – a (pseudo-) random number and the current time in seconds. The engineID is only for SNMP users (i.e. SNMP get/set/walk commands). ~~The trap users are generated on the receiving end (SNMP~~

~~Manager) with their own engineid and the traps should be configured with those.~~

**Status update (July 2019)**

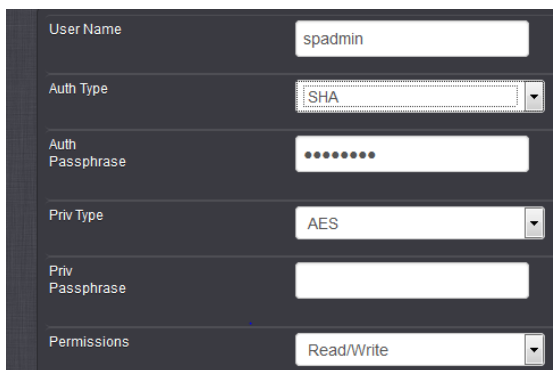
➤ update version 5.8.5 update now retains engine ID on each startup

- **per the 5.8.5 release notes:** “Corrected behavior of SNMP in order to retain engine IDs on each startup.”

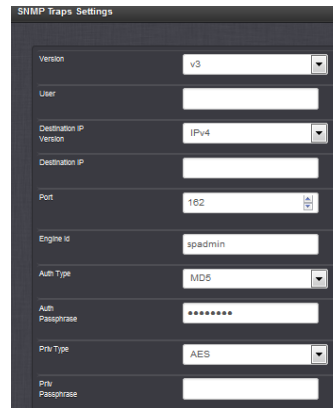
Q SNMPv3 Users - it appears one can only make auth/priv users (no noauth,nopriv ones).

**A Keith's response:** Correct. SecureSync is authpriv only. You can set Permissions in the snmpV3 section of the **Management -> SNMP Setup** page of the browser, to read or read/write (as shown in the screenshot below). If the user wants to setup the 'Trap only' user, it does not have to be reflected on the SecureSync and will need to be setup on the receiving end (SNMP Manager). The SNMP traps section of the Management -> SNMP Setup page of the web browser can configure those users. They essentially will have noauth and nopriv on SecureSync, since they are used to login to the snmptrapd remote service on the receiving end.

**Users for SNMP gets**



**Users for Traps**



Q I have a Customer who wants such accounts. If this capability is eliminated as a security lockdown, please let me know and I'll pass it along.

**A Keith's response:** I believe the reason that noauth/nopriv is not supported is because it's an unsecure connection (if a secure connection isn't a concern, can just use SNMPv1/v2c. No need to use SNMPv3).

---

**“User name” field**

- **Versions 5.2.1 and above:** can be **1 to 31 characters** (refer to Mantis case 2923). Used to be 8 to 32 characters in earlier versions.
- **Versions 5.2.0 and below:** can be **8 to 32 characters** (earlier rev user Manual incorrectly states “Between 4 and 32 characters in length”)

**A) Classic interface browser: “Notifications (traps)” tab**

**User/Community field:** minimum of 4 characters

SNMP SETUP										
		General Setting		Communities (v1/v2c)		Users (v3)		Notifications (Traps)		
Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
v2c	Trap	snmptest	IPv4	10.2.100.124	162		None		None	
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	

### Setting up ManageEngine SNMP Manager to work with SNMPv3 traps from SecureSync

1. In the **Management** -> **SNMP** page of the SecureSync, Add/Configure a new V3 user (note this is not required to send a v3 trap that wireshark can see, but is required for the SNMP manager to be able to authenticate/see the trap). Use the same user name that is used for the V3 user name (example below uses "rererere")

The dialog box titled "SNMP V3 Settings" contains the following fields:

- User Name:
- Auth Type:
- Auth Passphrase:
- Priv Type:
- Priv Passphrase:
- Permissions:

A "Submit" button is located at the bottom right.

2. Select "V3" at the top of the top of the "General tab" of the ManageEngine GUI

The "MibBrowser Settings" dialog box has tabs for "General", "Template Settings", and "Mib Settings". Under the "General" tab, the "SNMP Version" section shows three radio buttons: v1, v2c, and v3. The v3 radio button is selected.

3. Select the checkboxes for both "Save V3 Settings to file" and "Set EngineID for adding V3 entry"

The "V3 Settings" section of the dialog box contains the following options:

- Save V3 Settings to File
- Set EngineID For Adding V3 entry
- Save V3 Settings to Database

A "Database Settings" button is located to the right of the checkboxes.

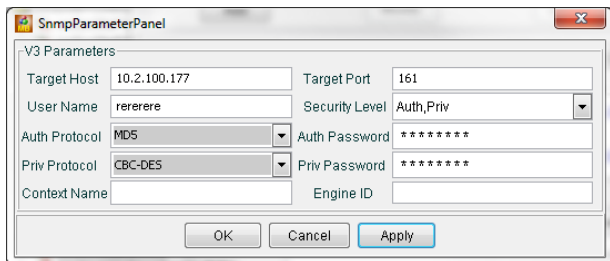
4. Press the "Add" button in the bottom left corner to add a "v3 user"

User...	Secur...	Auth ...	Priv P...	Auth ...	Priv P...	Targe...	Targe...	Engin...	Entity
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>									
<input type="button" value="Restore Defaults"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>									

5. Enter the IP address of the SecureSync, the SNMPv3 username and change Security level to Auth,Priv. Change the Auth and Priv protocols as necessary and enter the Auth and Priv passwords to match the settings in the



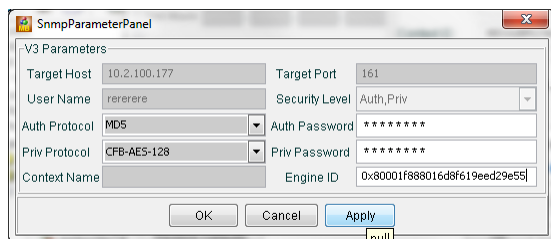
SecureSync. Then press Apply (note the context name and engine id will still be blank at this point).



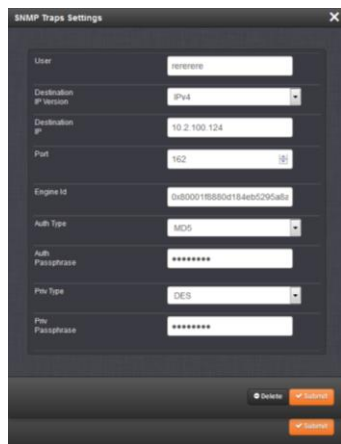
- With Auth and Priv protocols and passwords matching the SecureSync's SNMPv3 user section, the context ID field in the main page (General tab) of the manageengine gui will be generated.



- Copy/paste this entire context value into the "engineID" field of the sub-menu (press the "modify" button at the bottom to re-open it).



- Create a SNMPv3 trap in the SecureSync, using the same values that are used in the SNMP user. Also paste the context ID in the manageengine GUI into the "Engine ID" field of the SNMPv3 trap pop-up menu and submit.



## A) SNMPv1 and SNMPv2c

### SNMP Community/User field

- Versions 5.2.1 and below:** Can be **8 to 32** characters (SecureSync Manual incorrectly stated "between 4 and 32 characters in length.")
- Versions 5.3.0 and above:** Can be **1 to 31** characters (refer to Mantis case 3103). Note this change was supposed to be in the version 5.2.1 update, but it wasn't included.

## SNMP v1/v2C trap destination port number:

- Factory Default SNMP trap port value is port 162

### (5.6.0 and below only) Limitation of available port numbers

- Update Version 5.7.0 increased the port restriction range:
  - [JIRA Ticket SSS-271] - SNMP Trap Port restriction should be **0-65535**, instead of 0-1023

**(v4.7.0 and below only) 6/28/11 KW-** In all versions prior to version 4.7.0, the SNMP trap destination value wasn't displayed or able to be changed in the web browser. It was set to port 162 without the ability to change it to another desired value.

Besides updating the software to a newer version, a work-around allowed the port value to be changed via the CLI.

### Email DL sent to Todd Belcher on 6/27/11

Hello Todd,

I have some information for you. It is a description of how you can work around the bug and still send traps to a different port.

- 1) Log in to the unit via the command line (telnet, SSH, or serial port on front panel) as 'spadmin'
- 2) Change directory into the config directory (cd config)
- 3) Edit the snmpd.conf file using vi (vi snmpd.conf)
- 4) Find the "trapsess" line in the configuration file and change the port to the desired value.
- 5) Save the file (:wq)
- 6) Disable/enable SNMP from the Web UI.

If you do not know how to use 'vi', then you will need to ftp the file off the unit, change the port with an editor you know how to use, then ftp the file back onto the unit.

## Deleting a value from the Network -> SNMP Setup page, Communities tab

Q When we are configuring the SNMP Communities (1v/2vc), I accidentally enter an IP address into "IPv4 Network Access" field and I would like to remove the IP address. However, I am not able to remove the IP address. Please assist if this is a bug or normal behavior. Please do also advice how I can remove the unwanted IP address in the "IPv4 Network Access" field. Thus, please assist to check with Spectracom and reply asap.

A. **Keith's response:** I was able to enter a value in this field and then able to delete it. But in order to delete the value, I needed to change the "Permission" field in the same row to the default value of "None". Then, I removed the value from the field and hit Submit. The value was no longer present. Until I changed this field to "None", it wasn't clearing the field. Please have your customer change the value to "None", delete the value and hit Submit.

**(Network -> SNMP page, Notifications tab) SNMP "Version" field displays a Null" when SNMPv3 is selected (applicable to classic interface only):**

- (Reference Mantis case 1909) at least versions 4.8.7 and below.

Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
v1	Trap	trap	IPv4	10.2.100.29	162		None		None	
	Trap	snmpdtest	IPv4	10.2.100.29	162	0x80001f8880	MD5	snmpdtest	DES	snmpdtest

## SNMPd config file

- Path to the snmpd.conf file in the time server: home/spectracom/config
- For more info, refer to: <http://www.net-snmp.org/docs/man/snmpd.conf.html> and <http://www.net-snmp.org/wiki/index.php/Vacm> (VACM info)

snmpd supports the View-Based Access Control Model (VACM) as defined in RFC 2575, to control who can retrieve or update information. To this end, it recognizes various directives relating to access control.

**“com2sec”**  
V1 and v2c user  
community names

**“Group”**  
Defines v1/v2c  
users as either v1 or  
v2c

**“Access”**  
Group access  
control (read/write)

**SNMP V3  
users**

**“System Group”**  
System  
information

```
spectracom@spectracom111 ~$ cd config
spectracom@spectracom111 ~$ cat snmpd.conf
#-----
#com2sec sec.name source community
#-----
com2sec comuser 3 default snmptestAlpha
com2sec comuser 4 default snmptest
#-----
#group groupname sec.model sec.name
#-----
group rwnoauthgroup v2c comuser 3
group rwnoauthgroup v2c comuser 4
group rwprivgroup usm snmpv3test
group rwprivgroup usm snmpv3user
#-----
#view name incl/excl subtree mask
#-----
view all included .1
#-----
#access name context sec.model sec.level prefix read write notify
#-----
access rwnoauthgroup "" any noauth exact all none none
access rwnoauthgroup "" any noauth exact all all none
access roauthgroup "" any auth exact all none none
access rauthgroup "" any auth exact all all none
access rwprivgroup "" any priv exact all none none
access rwprivgroup "" any priv exact all all none
#-----
#createUser username [MD5|SHA] [passphrase] [DES] [passphrase]
#-----
createUser snmpv3test MD5 123456784343434 AES 12345678434343434
createUser snmpv3user MD5 12345678 AES 12345678
#-----
#trapsess [SNMPCMD_ARGS] host
#-----
#-----
#agentX configuration
#-----
master agentX
agentXPerms 770 770 spui root
agentXSocket tcp:localhost:705
agentXTimeout 1 # This is the default
agentXRetries 5 # This is the default
#-----
#system group
#-----
sysObjectID 1.3.6.1.4.1.18837
sysContact techsupport@spectracomcorp.com
sysLocation Unknown
sysDescr Spectracom Product
sysServices 72
#-----
#miscellaneous
#-----
agentgroup root
agentuser spui
authtrapenable 2
spectracom@spectracom111 ~$
```

---

## \*\*\*SysObjectID, SysContact and SysLocation fields

### SysObjectID

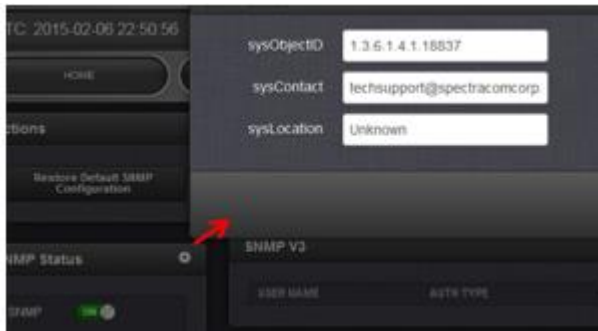
- **SysObjectID:** The three values can be changed from the default values if desired.

#### **Issue: Changing SysObjectID isn't propagating through SNMP.**

**Note:** This appears to be an issue with at least version 5.2.0 and below. Refer to Mantis 2973 (Changing it doesn't appear to be propagating all the way through SNMP)

(Status update, 23 Apr 15). It appears Mantis 2973 is being fixed in the version 5.2.1 update.

1. Click on **Gear** icon next to **"SNMP Status"**



---

### SysLocation field

**Issue:** in at least software versions 5.3.0 and below, this field just accepts letters and numbers (no spaces or symbols such as hyphens, underscore etc). I added Mantis case 3119 to look into this.

---

### SysName field (unit's hostname in SNMP)

- Was made configurable (Mantis case 3095) in version 5.3.0 (I believe)
  - Wasn't a user-configurable field in earlier versions of software.
- This field reports the assigned hostname.
- This field is only updated when the unit is rebooted, or if SNMP is stopped/restarted. If DNS changes the name thereafter, SNMP can be stopped/restarted for the new name to be updated.
  - Keith added Mantis case 3099 to have it change automatically, but Dave Sohn responded it's working as it should. SNMP won't see the change until SNMP is restarted.

---

### Ability to enable/disable SNMP via the CLI interface

Q. (from Wade Sober) Is there a way to enable SNMP through the command line interface on SecureSync?

**A. Reply from Dave Sohn (10/29/12)** There is no planned mechanism to enable SNMP directly via the CLI. We are adding the capability to save and restore configurations via the CLI, which would include SNMP. Those configurations could be used as a "golden" configuration to be loaded on deployed units.

**Update for this question:** Archive Version 4.8.9 added SNMP (and NTP) to the CLI "serv" command. Starting with version 4.8.9, SNMP can be stopped or started using the **servset** command (SNMP status can be read using the **servget** command).

---

## Verifying if SNMP and SNMPSAD are both running

To see if a particular process (such as SNMPSAD and SNMPSAD, our sub-agent) is running, type `ps -el | grep snmp` <enter> (where it will list everything with the name typed after “grep”):

```
Spectracom spectracom # ps -el | grep snmp
5 S 1001 2923 1 0 80 0 - 1973 poll_s ? 00:00:01 snmpd
5 S 0 2940 1 0 80 0 - 1989 poll_s ? 00:00:00 snmpsad
Spectracom spectracom #
```

**Note:** when the SNMP enable/disable switch is off, both snmpd and snmpsad should be stopped (not listed)

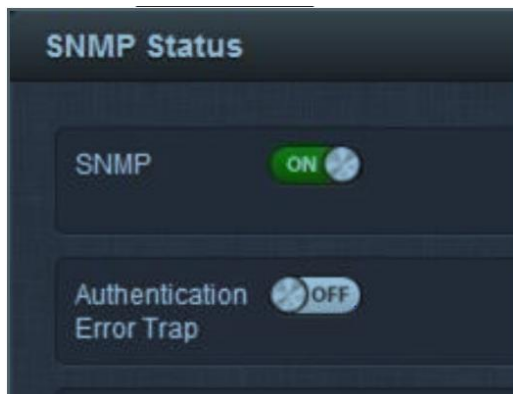
---

## Auth Error trap (“SNMP Authentication Error” trap)

- The Auth trap is not associated in any way with web browser or CLI interface login.
- The Auth trap is sent when there is an SNMP Authentication error on an SNMP query (such as a Get)
- To test this trap, enable SNMP, the Authentication trap, and a trap receiver. Attempt an “SNMP Get” to the unit using an incorrect community or user to see the trap being sent.

The majority of the events that can send an SNMP trap are on the [Management](#) -> [Notifications](#) page of the browser (in the **Timing**, **GPS** and **System** tabs).

The Authentication Error trap is enabled in a separate location than the others (and it’s disabled by default). It’s on the left-side of the [Management](#) -> [SNMP](#) Setup of the browser (just below the SNMP On/Off switch as shown below:

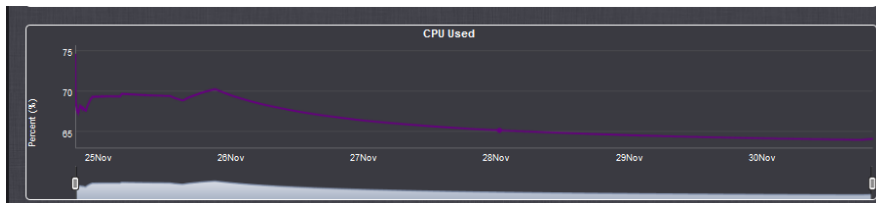


## CPU usage (CPU used) / Processor usage/CPU usage 100%

- Refer to Mantis case 3029.
- CPU usage is a comparison of processor “use time” versus “rest time”.
  - CPU usage is high (especially in versions prior to v5.4.1) in the SecureSync because ETX is a single core processor running multiple threads.
  - In version 5.2.0, CPU usage is running around 85 to 90%. After downgrade to version 5.1.2, similar values still being reported (around 91%). Upgrade to version 5.3.1 reduces CPU usage to around 70% or so due to making software run more efficiently. Upgrade to v5.4.1 reduces our CPU usage to around 50% or so.
  - Though the CPU usage is high, NTP is the one of the higher priority threads. So NTP performance is NOT affected in any way by the high CPU usage.

### CPU usage graph and raw data (software versions 5.3.1 and above)

- CPU usage graph was added in **version 5.3.1**
- Located at the bottom of the **Tools ->System Monitor** page of the newer browser (not available in classic interface).
- Graph data is captured/obtained/logged about once a minute, SO a high burst of short duration CPU activity might NOT be registered on the Log graphs/data for the database, but still occur.



### Issue with Graph data display: Fix in v5.8.7 update to address an error in the data being displayed in the graph

- Versions 5.8.6 and below were averaging the CPU usage data since the last boot-up.
- Version 5.8.7 (and above) update fixes this by reporting the raw data, instead of the running average.
- Refer to JIRA ticket SSS-745 – “CPU utilization in system monitor is averaged across the entire uptime of the device.” See excerpt below:

Projects / SecureSync Sustainin... / SSS-745

#### CPU utilization in system monitor is averaged across the entire uptime of the device

Attach Create subtask Link issue

**Description**

Pointed out to be suspicious by @Ryan Johnson, the cpu utilization in the webui is **not** the utilization from minute-to-minute, but rather the average utilization since boot.

This means that the longer a system is running, the less useful the data is - of course. This should probably be reporting the cpu utilization since the last data point.

I recommend using `/proc/stat` as in these solutions here:

- <https://stackoverflow.com/questions/23367857/accurate-calculation-of-cpu-usage-given-in-percentage-in-linux>
- <https://unix.stackexchange.com/questions/27076/how-can-i-receive-top-like-cpu-statistics-from-the-shell>

**Functional Test Procedure**

None

## Raw data for the CPU usage graph

- The raw data for the graph is stored in the SQLite database (part of the log bundle (Refer to the [MySQL section](#) in this doc for additional info on the database).
  - Data for this graph is located (can be viewed) in the “**log\_sys\_mons**” table, “**cpu\_used**” column
  - CPU usage is captured about once a minute (at about the 30 second mark). SO a high burst of short duration CPU activity might NOT be registered on the Log graphs/data for the database, but still occur.

	load01	load02	load03	mem_used	disk_used	kb_read_s	rb_wrtn_s	kb_read	kb_wrtn	cpu_used	sys_temp	cpu_temp
1	1.41	1.4	13.011516785...	48	0.02	0.0	65157.0	253375628.0	57.35	78	89.625	
2	1.34	1.38	13.122969544...	48	0.02	0.0	65157.0	253449924.0	57.35	78	89.625	
3	1.34	1.38	13.457327821...	48	0.02	0.0	65157.0	253526588.0	57.35	78	89.625	

## Reading CPU usage for all Versions of SecureSync software: .1.3.6.1.2.1.25.3.3.1.2

Type: **watch -n1 snmpwalk -t5 -v 2c -c snmpstat 10.2.192.226 .1.3.6.1.2.1.25.3.3.1.2**  
(updates once-per-second)

```
spadmin@Spectracom111 ~ $ snmpwalk -t 5 -v 2c -c snmpstat 10.2.100.177 .1.3.6.1.2.1.25.3.3.1.2
HOST-RESOURCES-MIB::hrProcessorLoad.196608 = INTEGER: 86
```

Note: Software Versions 5.2.1 and above can also use the following OIDs:

- percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0
- raw user cpu time: .1.3.6.1.4.1.2021.11.50.0
- percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0
- raw system cpu time: .1.3.6.1.4.1.2021.11.52.0
- percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0
- raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0
- raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

## Linux vmstat and vmstat 1 CLI commands

- Refer to sites such as: [http://linuxcommand.org/man\\_pages/vmstat8.html](http://linuxcommand.org/man_pages/vmstat8.html)

**Vmstat** reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length *delay*. The process and memory reports are instantaneous in either case. **vmstat** (one time) and **vmstat 1** (continuous output)

```
spadmin@Spectracom111 ~ $ vmstat
procs -----memory----- --swap-- -----io----- -system-- -----cpu-----
 r b swpd free buff cache si so bi bo in cs us sy id wa st
 1 0 0 326564 21692 81696 0 0 1 13 297 256 57 34 10 0 0
spadmin@Spectracom111 ~ $
```

## FIELD DESCRIPTION FOR VM MODE

### Procs

r: The number of processes waiting for run time.

**b:** The number of processes in uninterruptible sleep.

### Memory

**swpd:** the amount of virtual memory used.  
**free:** the amount of idle memory.  
**buff:** the amount of memory used as buffers.  
**cache:** the amount of memory used as cache.  
**inact:** the amount of inactive memory. (-a option)  
**active:** the amount of active memory. (-a option)

### Swap

**si:** Amount of memory swapped in from disk (/s).  
**so:** Amount of memory swapped to disk (/s).

### IO

**bi:** Blocks received from a block device (blocks/s).  
**bo:** Blocks sent to a block device (blocks/s).

### System

**in:** The number of interrupts per second, including the clock.  
**cs:** The number of context switches per second.

### CPU (These are percentages of total CPU time)

**us:** Time spent running non-kernel code. (user time, including nice time)

**sy:** Time spent running kernel code. (system time)

**id:** Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time. **(Note: CPU usage is the inverse of this value. So if the idle is 15, the usage is 85%)**

**wa:** Time spent waiting for IO. Prior to Linux 2.5.41, shown as zero.

---

### CPU usage 100% (100% CPU usage)

#### Possible causes (functions associated with ETX/eth0)

1. **Failed logins occurring** (review the auth.log)
2. **SNMP issues** (refer to Salesforce Cases such as 233777)
  - Associated segfaults were asserted in keern.log
  - SNMP configs may be corrupt (such as after uploading a saved config bundle)



## \*\*Using Linux to perform SNMPWalks SNMPGets SNMPTraps

- Note: To perform an SNMPwalk, SNMPget or receive traps in linux, use another SecureSync

(Note: This is also available as **spadmin**. So customers are able to use one SecureSync to hit another one via SNMP)

**Important note:** Make sure that the SecureSync being used to get in to the destination SecureSync is configured in the Destination SecureSync an SNMP user (or use IP address value of **default**) as shown below:

VERSION	GROUP NAME	COMMUNITY	IP VERSION	IP ADDRESS
v2c	Read/Write	snmptest	IPv4	default

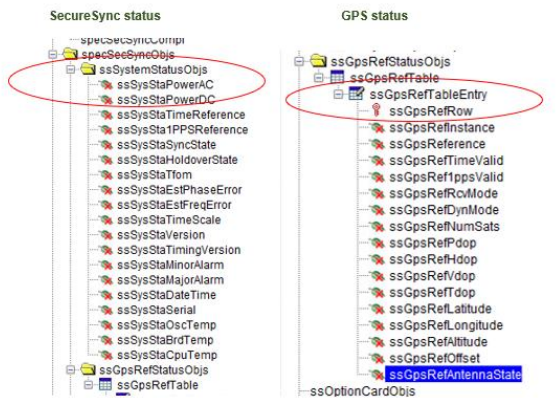
- Refer to: <http://en.wikipedia.org/wiki/Net-SNMP>

[https://docs.oracle.com/cd/E19201-01/820-6413-13/SNMP\\_commands\\_reference\\_appendix.html#50446362\\_54136](https://docs.oracle.com/cd/E19201-01/820-6413-13/SNMP_commands_reference_appendix.html#50446362_54136)

**Note:** You can also perform SNMPgets on a SecureSync (via its own CLIU interface), by using its own IP address, in the SNMPget commands.

## Using **snmpget** command versus using **eithersnmwalk/snmpgetnext** commands (for retrieving values from an SNMP tables)

- **snmpget** command is for SNMP OIDs *stored in a folder*
- **snmpwalk** (or **snmpgetnext**) commands is used for for SNMP OIDs *stored in an SNMP table (such as GPS receiver objects)*



**email below, Keith sent (5 Dec 2020)**

At the command prompt, perform the following command to successfully read the current Antenna Sense: **snmpwalk -v 2c -c XXXXXXXX Y.Y.Y.Y 1.3.6.1.4.1.18837.3.2.2.2.1.1.17.0 <enter>** (where **XXXXXXX** is the v2c community name, and where **Y.Y.Y.Y** is the SecureSync's IP address).

Below is an example command, and the expected response: (Note the first word is **snmpwalk**, instead of the usual word **snmpget**)

```
snmpwalk -v 2c -c snmptest 10.15.108.12 1.3.6.1.4.1.18837.3.2.2.2.1.1.17
```

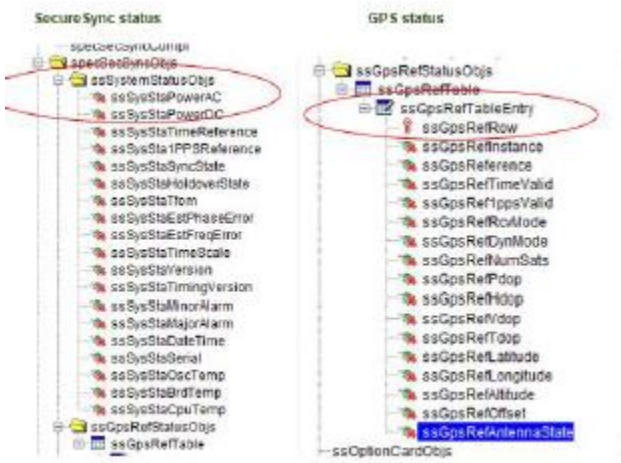
```

spadmin@Spectracom ~ $ snmpwalk -v 2c -c snmpptest 10.15.108.12 .1.3.6.1.4.1.1883
7.3.2.2.2.1.17
SNMPv2-SMI::enterprises.18837.3.2.2.2.1.17.1 = INTEGER: 3
spadmin@Spectracom ~ $

```

Here is the explanation why the command needs to be snmpwalk, instead of snmpget (based on my testing)

Below are two excerpts from an SNMP Manager GUI interface. The objects on the left (general SecureSync status messages, such as TFOM for instance) are listed under a folder. The objects on the right (for GPS/GNSS status) are listed in an SNMP table.



When polling objects stored in an SNMP table (instead of a folder), the SNMP manager knows how to use an “snmpget” command to poll an object from the table. This results in a successful return of the value (as shown below, and like you are successfully observing at your facility):



However, when polling a value directly from an SNMP table, a standard snmpget command will apparently have an issue retrieving the value from the SNMP table (as shown below):

```
spadmin@Spectracom ~ $ snmpget -v 2c -c snmpstest 10.15.108.12 .1.3.6.1.4.1.18837
.3.2.2.2.1.1.17
SNMPv2-SMI::enterprises.18837.3.2.2.2.1.1.17 = No Such Instance currently exists
at this OID
spadmin@Spectracom ~ $
```

But by just changing the same command from “snmpget” to “snmpwalk” . The retrieval of the value is then successful:

Below is the info I found online, which caused me to change the command from **snmpget** to **snmpwalk** (and it worked)  
<http://etutorials.org/Networking/network+management/Part+II+Implementations+on+the+Cisco+Devices/Chapter+4.+SNMP+and+MIBs/MIB+Table+Retrieval+Example/>

The snmpwalk utility initiates a series of SNMP GetNext operations, one per polled managed object:

```
SERVER % snmpwalk -c public -v 2c router ifTable
RFC1213-MIB::ifIndex.1 = INTEGER: Ethernet0/0
RFC1213-MIB::ifIndex.2 = INTEGER: Serial0/0
.....
```

Based on the wording in this website, I also just tested the **snmpgetnext** command (instead of using snmpget or snmpwalk) and this command will **also** successfully return a value from a table:

```
spadmin@Spectracom ~ $ snmpgetnext -v 2c -c snmpstest 10.15.108.12 .1.3.6.1.4.1.1
8837.3.2.2.2.1.1.17
SNMPv2-SMI::enterprises.18837.3.2.2.2.1.1.17.1 = INTEGER: 3
```

In summary, your customer should replace the word **snmpget** in the commands to obtain GPS receiver status, with either **snmpgetnext** or **snmpwalk** to obtain the antenna sense, because this GPS value is stored in an SNMP table.

## Example SNMPGets:

### General info

#### A) Desire to perform repeated SNMP Gets (same get repeatedly)

Use the “**watch -n**” command at the beginning to perform the SNMPGet command repeatedly

- Use linux “**watch -n**” before the snmpget command

(Example to run once per second): **watch -n1 snmpget -v 2c -c snmpstest 10.15.108.11 1.3.6.1.4.1.18837.3.3.2.1.0**

**Note:** the time at the top will increment each second

#### B) SNMPv3 gets (to add timeout “-t 5”)

(type) **snmpget -v3 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.100.177 .1.3.6.1.4.1.18837.3.3.1.1.0**

### Continuous SNMPv3 gets

(type) **watch -n 1 snmpget -v3 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.100.176 .1.3.6.1.4.1.18837.3.3.1.1.0**

#### C) SNMPv3bulkget

(type) **watch -n 1 snmpbulkget -v3 -t10 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

### Example SNMPWalks:

- CTRL + C to stop the output (standard for Linux) (or hold left mouse button and slide mouse either left or right to pause).
- Reports OIDs and values only (not object names)
- Can walk from any point. Whatever portion of the Object number is entered, it will get everything after that value (such as 18837.3 will find everything after this number)
- Use the “watch -n” command at the beginning to perform the walk repeatedly

(Syntax): `snmpwalk -t 5 -mALL -v 2c -c public snmp_agent_ip_address sysobjectID`

#### 1. Walk the entire MIBs (with a 5 second timeout)

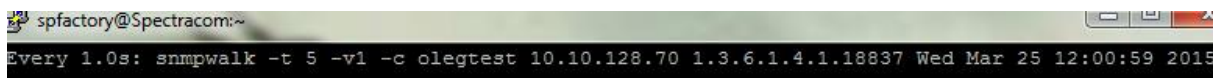
##### A) Just once

(Type): **snmpwalk -t5 -v2c -c snmpptest 10.2.192.226 1.3.6.1.4.1.18837**  
**snmpwalk -t5 -v2c -c snmpptest 10.15.108.12 1.3.6.1.4.1.18837**

##### B) Example to repeatedly walk the entire MIB, once per second:

(Type): **watch -n1 snmpwalk -t5 -v2c -c snmpptest 10.2.192.226 1.3.6.1.4.1.18837**

**Note:** the time at the top will increment each second

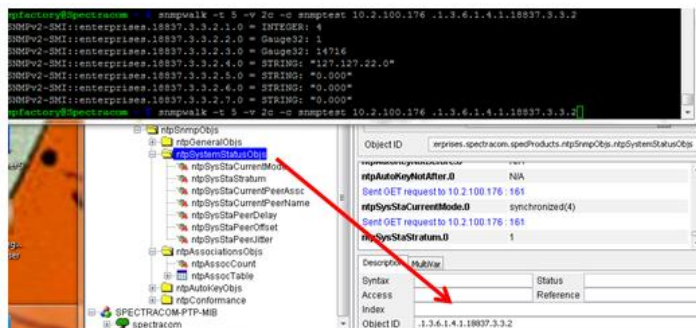


##### C) Walk just one MIB such as NTPSystemStatusObjsMIB (with a 5 second timeout)

(Type) **snmpwalk -t 5 -v 2c -c snmpptest 10.2.192.226 1.3.6.1.4.1.18837.3.3.2**

**Note:** -t10 is for a 10second timeout between each object)

**Note:** the numbers at the end of the snmpget (after the IP address) is the full OID number for the MIB file (see screenshot below for an example)



##### D) SNMPV3 walks

(type) **snmpwalk -v3 -t10 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

## E) Continuous SNMPv3 walk

(type) **watch -n1 snmpwalk -v3 -t10 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

(type) **watch -n 1 snmpwalk -v3 -t10 -u snmpv3test -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

## Specific SNMPgets

### A) Get the system uptime

(Type the following): **snmpget -v 2c -c snmpptest 10.15.108.11 SNMPv2-MIB::sysUpTime.0**

```

spadmin@Spectracom ~ $ snmpget -v 2c -c snmpptest 10.2.100.176 SNMPv2-MIB::sysUpTime.0
ISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (526358) 1:27:43.58

```

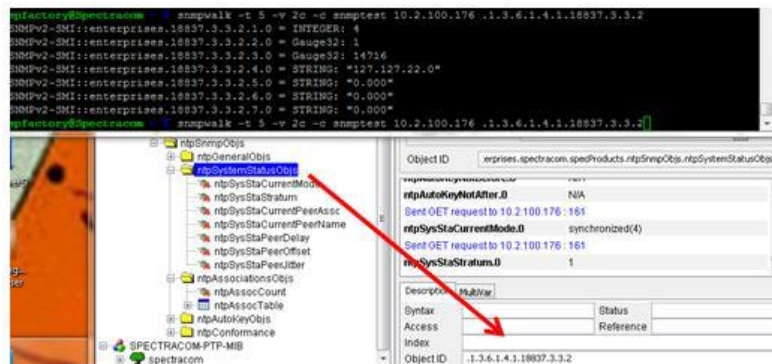
### B) Get the NTP's current status

(Type the following): **snmpget -v 2c -c snmpptest 10.15.108.11 .1.3.6.1.4.1.18837.3.3.2.1.0**

**Note:** the numbers at the end of the snmpget (after the IP address) is the full OID number, **plus a ".0"** added to the end.

### C) Retrieve GPS/GNSS info (such as Antenna sense)

- **Note:** GPS/GNSS objects are stored in an SNMP table (instead of a folder). Instead of using snmpget commands, use either snmpwalk or snmpgetnext commands to obtain GNSS info



- For details, refer to section further above "Using snmpget command versus using ethersnmwalk/snmpgetnext commands (for retrieving values from an SNMP tables)"

Antenna Sense ("ssGpsRefAntennaState")	.1.3.6.1.4.1.18837.3.2.2.1.1.17	spe
# Satellites being tracked ("ssGpsRefNumSats")	.1.3.6.1.4.1.18837.3.2.2.1.1.8	spe
GPS Time validity ("ssGpsRefTimeValid")	.1.3.6.1.4.1.18837.3.2.2.1.1.4	spe
GPS 1PPS validity ("ssGpsRef1ppsValid")	.1.3.6.1.4.1.18837.3.2.2.1.1.5	spe
GPS latitude ("GpsRefLatitude")	.1.3.6.1.4.1.18837.3.2.2.1.1.13	spe
GPS longitude ("ssGpsRefLongitude")	.1.3.6.1.4.1.18837.3.2.2.1.1.14	spe
GPS Altitude ("ssGpsRefAltitude")	.1.3.6.1.4.1.18837.3.2.2.1.1.15	spe

```

spadmin@Spectracom ~ $ snmpgetnext -v 2c -c snmpptest 10.15.108.12 .1.3.6.1.4.1.18837.3.2.2.1.1.17
SNMPv2-SMI::enterprises.18837.3.2.2.1.1.17.1 = INTEGER: 3

```

## SNMP Reboot command

- SNMP OID / Object to reboot (ssSysCtrlCommand)

**Note:** ssSysCtrlCommand was added in software version 4.8.8. Not available in versions 4.8.7 and below.

**Note:** This is the same command used to perform software updates via SNMP.

OID	Name	Function	Value to "Set"
18837.3.2.2.5.1	ssSysCtrlCommand	Either Reboot or apply remote software updates	"4" to reboot (SNMP Get will normally return "idle (1)". Values 2 and 3 are for performing software updates)

## Ability to enable/disable SNMP via the CLI interface

- Use the servset/servget CLI commands (available in versions 4.8.9 and above)

Q. (from Wade Sober) Is there a way to enable SNMP through the command line interface on SecureSync?

A. **Reply from Dave Sohn (10/29/12)** There is no planned mechanism to enable SNMP directly via the CLI. We are adding the capability to save and restore configurations via the CLI, which would include SNMP. Those configurations could be used as a "golden" configuration to be loaded on deployed units.

**Update for this question:** Archive Version 4.8.9 added SNMP (and NTP) to the CLI "servget and servset" commands. Starting with version 4.8.9, SNMP can be stopped or started using the servset command (SNMP status can be read using the servget command).

## "Auth Passphrases" and "Priv Passphrases" fields no longer displayed as clear text

**Starting** in Archive version 5.0.0, the "Auth Passphrases" and "Priv Passphrases" fields (SNMP SETUP page of the browser -> Notifications and Users tabs) were changed to "password" fields so that these values are no longer displayed as clear text.

**Note:** (classic interface only) For enhanced security, the number of x's displayed in the fields (four) does not indicate the same number of characters in the actual password. Passwords can be longer than four characters, but only four x's will be displayed.

Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
v3	Trap	xxxxxx	IPv4	192.168.0.1	162	0x01	SHA	xxxx	AES	xxxx

## SNMPv3 (Secure SNMP)

### "EngineID" field

- Required for SNMPv3 traps
  - Not required/available for SNMPv3 Gets and Sets (not in SecureSync's User configurations)

### From Wikipedia:

The snmpEngineID has a length of 12 octets.

The first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by the Internet Assigned Numbers Authority (IANA). For example, if Acme Networks has been assigned {enterprises 696 }, the first four octets would be assigned '000002b8'H.

The remaining eight octets are determined via one or more enterprise-specific methods. Such methods must be designed so as to maximize the possibility that the value of this object will be unique in the agent's administrative domain. For example, it may be the IP address of the SNMP entity, or the MAC address of one of the interfaces, with each address suitably padded with random octets. If multiple methods are defined, then it is recommended that the first octet indicate the method being used and the remaining octets be a function of the method.

**Email from Dave Sohn (11/28/12)** The mib browser I used generated a hex context ID, which I then used as the engineID. It needs to be a hexadecimal number entered starting with "0x". If they don't enter anything, we will default it to "0x01".

**Email KW sent to a dealer** This is not a value calculated in, or by, the SecureSync. It's a 12 octet, hexadecimal value that needs to be externally created by a user and then entered into the SecureSync's web browser.

### EngineID not retained when SNMP restarted

- engineID now retained when restarting SNMP (v5.8.5 and above, July 2019)

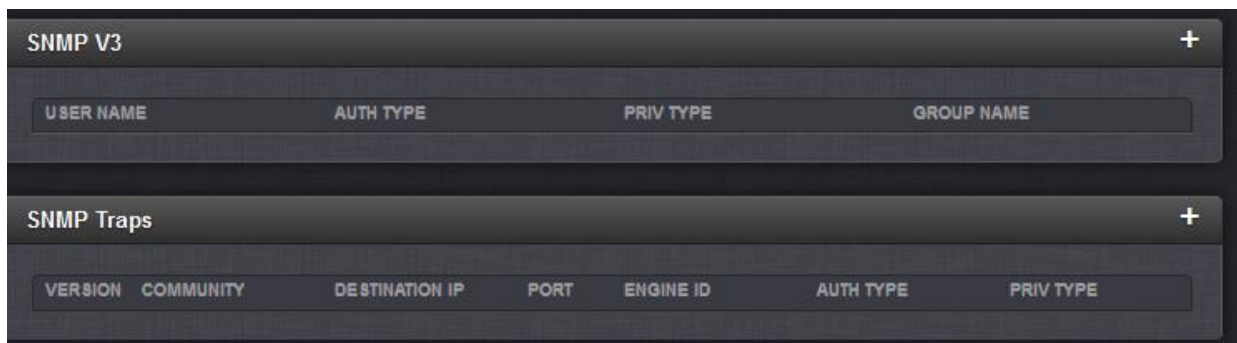
*Per the 5.8.5 release notes: "Corrected behavior of SNMP in order to retain engine IDs on each startup."*

---

### SNMPv3 encryption info/details

- Refer to Salesforce Cases such as 190594 and 192442

**Newer browser: Management -> SNMP Management** page of the browser, SNMP v3 and SNMP v3 Traps



### Access Control list for SNMPv3

Q On a separate note, I was asked to verify with you/Orolia if Access Control Lists can be written to restrict what Source IPs (SIPs) can access/pull SNMP data from the appliances.

A Email from Morgan to Ron Dries: Access Control List in relation to SNMP v3, which is not available, is the only way to do that with IP Tables? So under "SNMP V1/V2c Settings for Access", the IPv4 address provides access to SNMP if you have them listed correct? But this is no available to SNMPv3, that is the question they have.

A Replies from Ron Dries We have user configurable access rules:

[http://manuals.spectracom.com/SS/Content/NC\\_and\\_SS/Com/Topics/SETUP/AccessRules.htm](http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/AccessRules.htm)

The Access rules are not just for SNMP. Iptables could be used if they just want to restrict SNMP and leave the rest of the box open.

The IP address for v1/v2c configuration will tell SNMP in the SecureSync to only send data to a specific IP, or if default is used it will send a response to anyone.

SNMP v3 does not have this configuration available, so they could use access restrictions for the whole box, or possibly trying to create an iptables rule.

## Authentication type (AuthProtocol) / Privilege (privProtocol) terms

### A) “authPriv”: Messages can only be sent authenticated and encrypted

- newer (black/charcoal) browser (in at least v5.8.5 and below) enforces auth/priv configuraton (refer to “authNoPriv” below for more info).
  - “noAuthnoPriv”: Messages can be sent unauthenticated and unencrypted (**this mode is unsecure/not supported in SecureSync**)
  - “authNoPriv” Messages can be sent authenticated but unencrypted (this mode is not completely secure/not configurable via the newer web browser (in at least versions 5.8.5 and below). Note the classic browser does allow this configuration

### “AuthNoPriv” (in at least versions 5.8.4 and below)

#### Desire for new (black/charcoal browser) to support Auth

- Refer to JIRA Ticket (Feature Request) SSS-639
- Refer to Salesforce Case 194847
- newer browser in at least v5.8.4 and below does not allow Auth/NoPriv (its enforcing auth/priv
- temporary work-around is to configure SNMPv3 using classic interface browser (doesn't enforce auth/priv)

### B) Authentication (“Auth Type” field)

- **Auth Type:** supports **MD5** or **SHA** (no selection available for ‘none’)

## Encryption algorithms supported (“Priv Type” field): DES or AES

### AES support (such as AES 128-bit, AES 192-bit, AES 256-bit) with the Net-SNMP software package

- Refer also to the **Net-SNMP WIKI**: <http://www.net-snmp.org/wiki/index.php/> ([http://www.net-snmp.org/wiki/index.php/Strong\\_Authentication\\_or\\_Encryption](http://www.net-snmp.org/wiki/index.php/Strong_Authentication_or_Encryption))

#### 1. As of at least versions 5.8.9, 5.9.0 and 5.9.1

- Net-SNMP is still at 5.6.2.1. AES is still 128 bit (AES-128 only).

#### AES is still 128 bit (AES-128 only)

- Refer to JIRA ticket **SSS-623**
  - Per Tim Hammer “SS1200 currently has a patched version of 5.6.2.1 and so only supports AES128.”
- Reference Salesforce Case Number **190594**

Per <https://stackoverflow.com/questions/32566585/does-net-snmp-support-aes-192-and-aes-256-encryption>

“Update in 2019: In Aug 2018, net-snmp 5.8 introduced support for such, please refer to [http://www.net-snmp.org/wiki/index.php/Strong\\_Authentication\\_or\\_Encryption](http://www.net-snmp.org/wiki/index.php/Strong_Authentication_or_Encryption) (excerpted below)”

Q Does Net-SNMP support AES192 or AES256?

A The short answer is **Yes**, starting with **release 5.8** AES193 and AES256 are an optional configure option. There are two separate parts to the long answer:

**Per Keith (11 Apr 2019)** Net-SNMP is currently at v5.6.2.1 (in at least versions 5.8.4 and below). So AES-192/AES-256 is not currently supported until we update to a newer version of net-SNMP



Status update to the above info (27 Apr 2020) **it appears SNMP is still currently v5.6.2.1 (we have not updated SNMP)**

### Status update for JIRA SSS-623 (27 Apr 2020)

- This JIRA ticket is still open

Katie.Schrack (February 7, 2020, 12:08 PM)

In looking at our SNMPv3 package, do we have to update the package, if so add this support. Otherwise do not do for SS1200.

This should be a part of Trust Code.

Ryan Johnson

April 15, 2020, 2:22 PM

Maybe the question is what key length the AES implementation we use is. In the webUI it just says "AES". Can we indicate the keylength (e.g. AES-128 or AES-256)? Same with SHA

---

## 2. As of at least Sept, 2017 (earlier info)

- AES is 128 bit (no plans to update to 256 bit): refer to [https://groups.google.com/forum/#!msg/ mailing.unix.net-snmp-users/V\\_uVWkWUQx4/mqneIC5jC1EJ](https://groups.google.com/forum/#!msg/ mailing.unix.net-snmp-users/V_uVWkWUQx4/mqneIC5jC1EJ) (written in 2010)
- **Net-SNMP only supports AES 128 bit, It does not support 192 or 256 bit.**
- **Refer to sites such as:** <https://stackoverflow.com/questions/32566585/does-net-snmp-support-aes-192-and-aes-256-encryption> : "Net-snmp does not support AES 192 or 256"
- and [http://www.snmp.com/snmpv3/snmpv3\\_aes256.shtml](http://www.snmp.com/snmpv3/snmpv3_aes256.shtml) "Some network devices, including most Cisco devices, support SNMP with 256 bit AES. Some other devices do not. The net-snmp agent does not support AES256 with SNMPv3/USM"

**Email from Dave Sohn (31 Aug 2017): As far as I am aware, our SNMP agent (net-snmp) supports AES-128 only.**

**Email from Dave Sohn (7 Feb 2013): The implementation we have now only supports AES-128.**

AES-192 and AES-256 were only presented in a draft IETF standard, but is not standardized. Some vendors like Cisco have included AES-192 and AES-256 based on the draft.

---

**Spectracom SecureSync will not allow entry of "default" in the IP field for SNMP settings. UI gives "Must be in IP address format"**

- **Update:** this condition was addressed in software update version 5.1.7

### Versions 5.1.6 and below only

**Email from Dave Sohn (17 Sept 2014)** This issue is still present. The issue occurs when changing an existing SNMP V1/V2 entry. The UI preloads the IP address field with "default", if the entry was not limited to a specific IP address on creation. The issue can be worked around by deleting "default" from the IP address field and leaving it blank. ~~This remains an open issue in our tracking system.~~

## SNMPv3 Engine ID field

### EngineID value changes after each reboot/each restart of SNMP

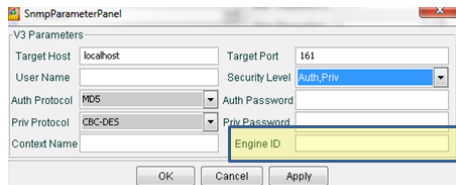
- Refer to Salesforce Cases such as **188893**
- Refer to JIRA ticket **SSS-258**
- Expected to be addressed in update v5.8.5

**Status Update.** Fixed in update v5.8.5 (Engine ID no longer lost when restarting SNMP)

*Per 5.8.5 release notes:* "Corrected behavior of SNMP in order to retain engine IDs on each startup."

### Obtaining "Engine ID" value using the ManageEngine software program

- 1) Main screen, Edit -> Settings, select "v3"
- 2) Select "engineID" for adding V3 entry"
- 3) Press "Add". "Engine ID" shown/entered in pop-up window



- 4) Enter this same value in the SNMPV3 EngineID field in the time server

**Note:** a default value may be entered automatically in this field. If not, can manually enter a value (such as "80001f8880d7c92a1f7ed4b50" for example)

### Number of available EngineID characters (field length)

- **Versions 4.8.9 and above:** 50 characters
- **Versions 4.8.8 and below:** 32 characters

---

## Obtaining unit's Model, Serial Number and version via SNMP

Summary of most recent status of these items (as of version 5.2.0, Feb 2015)

- **Model info:** Not available in versions 5.2.1 and below. Refer to Mantis case 1855.
- **Serial Number:** Added in update version 5.2.1 (April 2015). Not available in versions 5.2.0 and below. Refer to Mantis case 1855.
- **Installed software version (ssSysStaVersion):**
- **SecureSyncs:** Version 5.2.0 software now correctly responds with the installed version number (software versions 5.1.7 and below incorrectly responds with the word "Version" instead of the version number)
- **NetClock 9400s:** Version 5.2.0 still incorrectly responds with the word "Version" instead of the version number. Refer to Mantis case 2980.

### Earlier notes

- (13 Nov 2014) As of at least v5.1.7 and below, the Model Number is now available via SNMP (appears "NetClock 9483 and 9489" and SecureSync were added in 2010 MIB change) but the Serial Number still isn't available via SNMP (refer to Mantis Case 1855).

**Update:** Serial Number added as an available SNMP Get in v5.2.1 update

The SNMP OID for the Model Number is available via the Spectracom-Global-MIB.mib file.

(10/29/12) As of at least v4.8.7 and below, the Model and Serial Number are not available via SNMP (refer to Mantis Case 1855).

Q. Is the Serial Number and Hardware Version available via SNMP? If so, what OIDs should we use? We've looked through the provided MIBS, but didn't find anything.

**Note (11 Feb 15 KW)** Status update for the earlier answer below regarding Version info

The currently installed system version was added to the MIBS as "**ssStaVersion**" However, in versions 5.1.7 and below, it was incorrectly responding with the word "Version". Refer to Mantis case 2889.

### More recent:

- **SecureSyncs:** Version 5.2.0 software now correctly responds with the installed version number.
- **NetClock 9400s:** Version 5.2.0 still incorrectly responds with the word "Version" instead of the version number. Refer to Mantis case 2980.

**Note (13 Nov 14 KW):** Status update for the earlier answer below: The NetClock 9400 and SecureSync Model Number was added via a MIB file change in 2010. But at least versions 5.1.7 and below still don't provide Serial Number.

A. At this time, the Serial Number and Hardware Version information are not available via SNMP. The unit's Serial Number can be found on the Serial Number tag affixed to the appliance. We do not provide any "Hardware version" information. However, the "Software versions" for the various SecureSync modules can be obtained from the Tools/Versions page of its web browser.

**Note:** Post version 4.4.0 updates should have the Model/Serial Number at the top of the Tools/Versions page.

Note that the reported "Archive Version" is the "common reference" for all of the various software versions installed in the SecureSync. The "Archive version" defines all of the different versions of software installed. When a software update is applied to any of the various software modules, the "Archive Version" is updated, as well.

---

## SNMP for installed Option Cards

- As of May 2013, the only Option Card with SNMP functionality is the Model 1204-12 PTP Option Card.
- One of the six MIB files we send define OID for SNMP “gets” for the PTP Card (there are no available sets or traps for this Option Cards)

Q Are there any OIDs we can poll for the info about cards inserted in these devices?

A. **There are currently no SNMP OIDs associated with any of the Option Cards (there is no SNMP functionality associated with any the Option Cards nor is any planned at this time).**

**Update to this answer (7 May 13):** As mentioned in the bullets above, the Model 1204-12 PTP Option Card does have a dedicated MIB file for SNMP gets. As of at least Nov 2014, this is the only Option Card that has PTP functionality.

**Note** (as of at least Dec 2014, versions 5.1.7 and below) The PTP MIB file doesn't work with the 1204-32 Gb PTP card. It is only compatible with the 1204-12 10/100 PTP card.

---

## Desire to know if a network port is up or down

- Refer to the SecureSync SNMP Tech Note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP or to the NetClock SNMP tech note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\SNMP
- Web browser doesn't report the Operational state of a port (as of at least 4.8.9 anyways).
- Port state can be read using general SNMP MIB RFC 1213 (as of at least 4.8.9, a port being down is not available via a trap). We supply and support this generic MIB file.
- RFC 1213 MIB file contains an “iftable” (Interface table) with two fields that report port state. The admin field reports if the port is enabled and the Operational state field reports if the port is up or down.
- RFC 1213 MIB is not included in the SecureSync/NetClock 9483, but can be freely downloaded from sites such as: <http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=RFC1213-MIB>
- For more info on this file, refer to sites such as: <http://www.ietf.org/rfc/rfc1213.txt>

**Note:** There are more interfaces in the SecureSync and NetClock than just Eth0 (and Eth1-3 when the 1204-06 card is installed). The iftable sees more than just the four basic rear panel ports, but will report these other ones as being down. It was showing six ports instead of four, when I looked at this on a SecureSync with the Gigabit card installed.

---

## Desire to poll system disk, proc (processes) CPU usage and memory info

- Added ability to pull system memory, CPU, and CF card disk usage information from SNMP in software update version 5.2.1

Q. Is there an SNMP OID that reports free memory on these devices?

Update to the info below (23 Apr 15 KW) (version 5.2.1 is enabling new SNMP objects).

As of 5.2.1 the following system MIBs will be available:

### MEMORY:

Total Swap Size: .1.3.6.1.4.1.2021.4.3.0  
Available Swap Space: .1.3.6.1.4.1.2021.4.4.0  
Total RAM in machine: .1.3.6.1.4.1.2021.4.5.0  
Total RAM used: .1.3.6.1.4.1.2021.4.6.0  
Total RAM Free: .1.3.6.1.4.1.2021.4.11.0  
Total RAM Shared: .1.3.6.1.4.1.2021.4.13.0  
Total RAM Buffered: .1.3.6.1.4.1.2021.4.14.0

Total Cached Memory: .1.3.6.1.4.1.2021.4.15.0

**CPU:**

percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0  
raw user cpu time: .1.3.6.1.4.1.2021.11.50.0  
percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0  
raw system cpu time: .1.3.6.1.4.1.2021.11.52.0  
percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0  
raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0  
raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

**DISK USAGE:**

Path where the disk is mounted: .1.3.6.1.4.1.2021.9.1.2.1  
Path of the device for the partition: .1.3.6.1.4.1.2021.9.1.3.1  
Total size of the disk/partition (kBytes): .1.3.6.1.4.1.2021.9.1.6.1  
Available space on the disk: .1.3.6.1.4.1.2021.9.1.7.1  
Used space on the disk: .1.3.6.1.4.1.2021.9.1.8.1  
Percentage of space used on disk: .1.3.6.1.4.1.2021.9.1.9.1  
Percentage of inodes used on disk: .1.3.6.1.4.1.2021.9.1.10.1

**Earlier Email from Oleg (9 Dec 14)** You can run snmpwalk on the IP address, without including Spectracom MIB info. There should be system disk, proc and mem info.

**Earlier Email from Dave Sohn (9 Dec 14)** Some additional information is available through standard MIBs that are included with SecureSync. The hrStorageTable within the Host Resources MIB (RFC2790) is supported and can provide a snapshot of the memory usage within SecureSync.

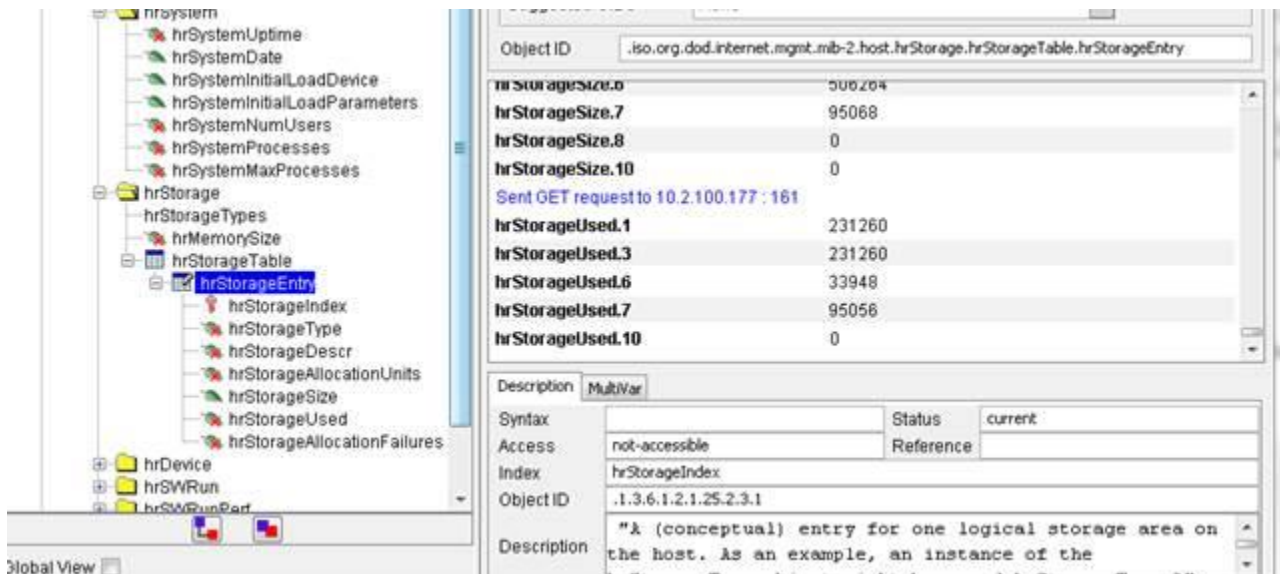
**Set**

	hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageAlloc...	hrStorageSize	hrStorageUsed	hrStorageAlloc...	Index Value
1	1	.1.3.6.1.2.1.25....	Physical memory	1024	506264	181668		1
2	3	.1.3.6.1.2.1.25....	Virtual memory	1024	506264	181668		3
3	6	.1.3.6.1.2.1.25....	Memory buffers	1024	506264	22564		6
4	7	.1.3.6.1.2.1.25....	Cached memory	1024	74312	74312		7
5	8	.1.3.6.1.2.1.25....	Shared memory	1024	0			8
6	10	.1.3.6.1.2.1.25....	Swap space	1024	0	0		10

**Keith's response to customer (9 Dec 14)**

I have some "late-breaking" information for you, that I wasn't previously aware of, regarding SNMP polling of free memory. I happened to mention your inquiry to our Engineering Manager and he provided me with this info below...

This free memory isn't currently available from any of the Spectracom MIBs or the generic SNMP MIB. However, it is available via the hrStorageTable within the Host Resources MIB (RFC 2790) which the SecureSync supports (see the screenshot below).



In order to see this value for myself, I initially tried compiling just this one MIB file. But there are dependencies to also compile the IF-MIB (RFC 2233) the SNMPV2-MIB (RFC 1907) and the IANAIFTYPE-MIB (RFC1573) files also. The compile order doesn't appear to matter (unless I happened to get lucky the first time ☺).

All of these files can be downloaded from various sites. But for your convenience, here is a link to the site I obtained all of them from: <http://www.ndt-inc.com/SNMP/MIBsByRFC.html>

## Spectracom PTP MIB file

- As of at least software version 5.1.7, the Spectracom PTP MIB file we provide with the other MIBS is only compatible with the 1204-12 10/100 Master/Slave PTP card. The PTP MIB file is not compatible with the 1204-32.

**Email from Keith (12 Dec 14):** Regarding the PTP Status tables, please be aware that the Spectracom PTP MIB file is only compatible with the Model 1204-12 10/100 Master/Slave PTP card. It is not compatible with the Model 1204-32 Gb PTP Master Option Card (there is no Spectracom MIB available for this particular PTP card). If the SecureSync has one or more 1204-32 cards installed and no 1204-12 cards, the table won't have any data and there will be no responses when polling the PTP objects.

## \*\*Testing/Verifying SNMP/Email alerts are enabled and working inside the SecureSync

### Testing SNMP traps and email alerts

#### 1. **sendtrap** and **sendtrap x** commands

- this more recent CLI command was added in v5.6.0
- Unlike testevent command, this command just sends test traps. It does not try to send any test emails.

#### 2. **testevent all** and **testevent x** commands

**Note:** The “**testevent**” command can be issued to send SNMP traps only! This command does not test email alerts. Refer to the SecureSync SNMP Tech note for more info on testing traps and email alerts

I believe the testevent may only work using v2 or v2c (not v1 or v3 - this is not confirmed)

#### 1. Versions 5.6.0 and above

- Update versions v5.6.0 added **sendtrap** and **sendtrap all** commands (in addition to earlier **testevent** command)

```
spfactory@Spectracom ~ $ sendtrap
Usage: sendtrap all
Usage: sendtrap <evtID> [evtID] [evtID] ...
 trapID: 1=Sync 2=Holdover
 3=Freq Error 4=Freq OK
 5=User Minor Alarm 6=User Minor Clear
 7=User Major Alarm 8=User Major Clear
 9=GPS Antenna 10=Minor Alarm
 11=Major Alarm 12=Reference Change
 13=1PPS Error 14=1PPS OK
 15=Hardware Error 16=Oscillator Alarm
 17=Oscillator OK 18=Reboot
 19=Minor Temp Alarm 20=Minor Temp Clear
 21=Major Temp Alarm 22=Major Temp Clear
spfactory@Spectracom ~ $
```

#### 2. Versions 5.5.1 and below

##### **testevent** and **testevent all** CLI commands

- Can include a number to send a specific trap using the testevent x command.
- Or send all available traps with the **testevent** command

The CLI allows spadmin account to perform various internal SNMP commands

```
spadmin@Spectracom /home/spectracom $ snmp
snmp-bridge-mib snmpdelta snmpnetstat snmptranslate
snmpbulkget snmpdf snmpset snmptrap
snmpbulkwalk snmpget snmpstatus snmpusm
snmpcheck snmpgetnext snmpstable snmpvacm
snmpconf snmpinform snmpptest snmpwalk
spadmin@Spectracom /home/spectracom $ snmp
```

I recommend using either **Wireshark** on a networked Windows PC, or **tcpdump** on the SecureSync (if its hasn't since been disabled) to verify whether a trap is being sent out of the SecureSync, on the correct ethernet interface (if the Model 1204-06 three port Gb Ethernet option card is installed) with each testevent command. This test eliminates the SNMP Manager and the associated MIBS from “the equation”. Either the traps are being sent out, or not sent out.

The SecureSync (versions 5.2.1 and above) has tcpdump utility installed, allowing the ability to “sniff” the ethernet

interface(s) of the SecureSync for any/all packets (such as SNMP traps) going out. Controlling tcpdump is via the CLI interface (an ssh or telnet connection):

(versions 5.2.1 and above only) Can use tcpdump in the CLI interface to see if snmp packets are being sent and which interface they are being sent from

- For additional info about using tcpdump to capture packets, refer to: [TCPdump \(wireshark for Linux\)](#)
  - Some examples below:

#### To capture data on specific Ethernet interfaces

- To capture traffic on **eth1** instead of default port of eth0: **sudo tcpdump -i eth1**
- To capture traffic on more than one interface (such as **eth0** and **eth1**): **sudo tcpdump -i eth0 -i eth1**
- To capture traffic on all interfaces **sudo tcpdump -i any**

#### To capture specific data type of packets (such as Radius packets only, snmp only)

Note-omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE

- **NTP** on eth0: **sudo tcpdump port 123** (no need to define interface as eth0 is default)
- **Radius** on eth0: **sudo tcpdump port 1812 and 1813** (no need to define interface as eth0 is default)
- **LDAP** on eth0: **sudo tcpdump port 389 and 636** (no need to define interface as eth0 is default)
- **Syslog** on eth0: **sudo tcpdump port 514** (no need to define interface as eth0 is default)
- **PTP** on eth0: **sudo tcpdump ports 319 and 320** (no need to define interface as eth0 is default)
- **SNMP Traps** sent to any Ethernet interface: **sudo tcpdump port 162 -i any**

```
spadmin@Spectracom ~$ sudo tcpdump port 162 -i any
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
21:20:11.907881 IP 10.2.100.176.52835 > roc-ops-kwing.int.croliia.com.snmptrap: C="snmptrap
" V2Trap(81) system.sysUpTime.0=269581 S:1.1.4.1.0=E:18837.3.2.3.0.2 E:18837.3.2.2.1.6.0=1
21:20:11.942491 IP 10.2.100.176.52835 > roc-ops-kwing.int.croliia.com.snmptrap: C="snmptrap
" V2Trap(101) system.sysUpTime.0=269584 S:1.1.4.1.0=E:18837.3.2.3.0.12 E:18837.3.2.2.1.3.0
=" " E:18837.3.2.2.1.4.0=""
^C
2 packets captured
```



## \*\*Troubleshooting / Known issues with SNMP

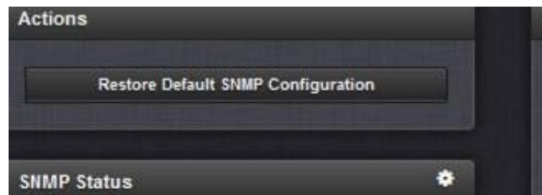
### A) General SNMP troubleshooting

In all cases when troubleshooting issues with SNMP → get a log bundle from the unit to review the **kern.log**, **cron.log**, **daemon.log** **snmpd.log** and **rexd.log** for SNMP entries and look for segfault in the kernel log (all of these logs are in the **home/spectracom/log** directory).

#### Potential fix to SNMP issues- reset just the SNMP configs

- Button in the upper-left corner of the **Management** -> **SNMP Setup** page resets just the SNMP configs
- Automatically restarts SNMP after reconfiguring.

In the upper-left corner of the **Management** -> **SNMP Setup** page of the newer (black/charcoal) web browser, there is a **“Restore Default SNMP Configuration”** button (as shown below). Unlike a **“clean”** which resets all of the configurations in the SecureSync, this particular button just resets the configs associated with SNMP. The engineer I'm working with recommended resetting and reconfiguring just the SNMP settings. Can you try this on at least one of the SecureSyncs and then try performing the **SNMPGet** command again? This button won't affect any of the other settings or operations besides SNMP.



If you don't mind trying this, please let me know if an **SNMPGet** or **walk** is successful after reconfiguring SNMP. Note there is no need to reboot the unit or to turn SNMP off and back on again before or after reconfiguring SNMP.

#### 1) Verify SNMP is Enabled via the web browser or CLI interface

- **New Web browser:** Management -> **SNMP Setup** page
- **CLI command:** **servget 7** <enter> ( to disable/enable **servset 7 off** **servset 7 on**)

```
spadmin@SpectraCom ~ $ servget 7
SNMP Service enabled
spadmin@SpectraCom ~ $
```

#### 2) SNMPWalk the SecureSync from itself (from the home/spectracom directory)

**Note:** Spadmin has permissions to do this.

**Note:** for the “address” at the end of the line, can use either **“localhost”** or **“127.0.0.1”**

```
spadmin
spadmin@SpectraCom /home/spectracom $ snmpwalk -v2c -c snmptest 127.0.0.1
```

```
spadmin@SpectraCom /home/spectracom $ snmpwalk -v2c -c snmptest localhost
```

These **SNMPWalk** commands should walk all of the objects in the SecureSync with a “running” display

#### 3) Perform an **“rc-status”**

Make sure **snmpd** and **snmpsad** are in the list and both indicate **“started”** (in green)

```
spadmin@Spectracom /home/spectracom $ rc-status
Runlevel: default
```

```
snmpd [started
snmpsad [started
```

- If snmp and/or snmpsad aren't listed in the response, SNMP isn't running. Go to the Management -> SNMP Setup page and see if the SNMP slider switch on the left side of the page is ON.
- If snmp and/or snmpsad indicate "crashed", SNMPD or SNMPSAD crashed. If SNMPD is crashed, likely need to update the SecureSync to version 5.2.1 (or higher). If SNMPSAD crashed, need to increase the timeout value in the device polling the SecureSync (no less than about 10 seconds) and should also update software to at least version 5.2.1.

#### 4) Perform a "ps -el | grep snmp"

There should be two red SNMP values in the response (**snmpsad** and **snmpd**)

```
spfactory@Spectracom ~ $ ps -el | grep snmp
5 S 0 16928 1 6 80 0 - 1990 poll_s ? 00:02:46 snmpsad
5 S 1001 16975 1 4 80 0 - 2029 poll_s ? 00:01:50 snmpd
spfactory@Spectracom ~ $
```

#### 5) Use tcpdump to verify if SNMP traps are being sent

➤ Note-omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

- Refer to the tcpdump section of this doc for more info
- SNMP Traps sent to any Ethernet interface:
  - (Versions 5.4.5 and above) **tcpdump port 162 -i any**
  - (Versions 5.4.1 and below) **sudo tcpdump port 162 -i any**

#### Example SNMPv3 traps with tcpdump (encrypted)

```
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
15:21:09.459717 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [!scoped FDDU]c5
ec_a0_af_3d_f3_e6_4e_0e_97_3f_03_e5_a9_fb_01_98_53_c8_32_aa_c1_05_03_2e_0b_69_3a_73_36_29_da_14_ac
43_4f_7d_72_c3_3e_70_07_37_bf_80_85_ac_4f_76_47_1a_0f_4b_5b_1c_88_05_f2_1b_3f_4c_25_cf_10_b4_fa_f
7_12_f8_59_a2_ee_5d_1c_91_35_91_1c_77_12_47_6b_2d_ec_54_53_f6_a3_8c_47_00_47_42_47_b3_a9_70_07_3f_
62_e7_5d_a7
15:21:47.189748 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [!scoped FDDU]f1
ae_cd_4c_c3_19_9a_8d_68_e8_f8_50_8a_83_cb_f0_29_65_c3_be_4d_46_86_a4_2f_55_b2_63_72_62_0d_b0_8a_3f
_17_85_e1_fa_21_cf_d5_77_ed_52_d3_ff_d8_0d_37_f0_6f_23_f1_86_95_2f_be_02_04_cb_24_12_29_02_b5_74_0
e_0d_8d_b1_93_1c_fa_bb_bd_43_41_bd_d3_9e_54_8d_10_a6_23_ba_c8_4c_43_ff_24_20_84_99_3c_c7_63_94_a5
ed_01_e9_2e
15:21:47.385695 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [!scoped FDDU]2e
79_70_5e_4b_cd_e5_a7_15_15_32_66_03_a8_0c_70_37_25_41_13_cd_65_8c_e2_50_0f_c7_34_2e_03_4c_47_88_d1
_1c_92_b5_c4_07_1a_89_9b_b0_3f_12_c2_be_5f_94_7f_2a_39_00_e2_e6_23_71_44_4b_ed_18_4c_e4_0a_e8_43_c
6_db_98_e6_45_9e_cf_4b_85_fe_16_3b_9d_36_e2_a6_d5_98_fa_72_bc_8e_38_9a_43_a3_2a_29_a1_ca_16_c8_ad
7c_01_b3_a4_ee_8e_ce_9b_35_5b_5d_10_c6_3d_0c_f5_40_86_65_72_b9_bc_b8_a1_4c_db_6e_6e_47_5d_fe_68
```

## B) Specific SNMP troubleshooting

### 1) SNMP Gets not working/timing out

- Make sure the configured "IP address" field (*Management -> SNMP Setup* page of the browser) is correct for the device performing the SNMP Get (or the field is set to "default", by leaving the field blank and submitting). If temporarily testing with another device besides the SNMP Manager, the configured IP address needs to be the PC used to test, or the field set to "default".

**Note:** The IP address field is a form of access restriction for SNMP. If the device trying to perform the SNMP Gets is not specifically the configured IP address, the device will not be able to perform SNMP Gets.

## 2) SNMPv1/v2c Traps not working/not being sent

- Make sure **Community name** value is correct correct (a trap is still sent to correct address, as observed with tcpdump)
- Make sure **Destination** value is correct (a trap is still sent when expected, but its sent to the wrong device, as observed with tcpdump)

## 3) SNMPv3 Traps not working

### Example SNMPv3 traps with tcpdump (encrypted)

```

listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
15:01:09.459717 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap 0="snmptrap" [Encrypted PDU]c5_
ec_a0_af_3d_f3_e6_4e_0e_07_3f_03_e5_a9_fb_01_95_53_c9_32_aa_c1_05_03_2e_0b_e9_3a_73_36_29_da_14_a2_
f_43_d7_72_c3_16_70_97_37_bf_80_e5_ac_af_76_67_1a_ef_45_1b_1c_88_05_f2_1b_31_4c_25_cf_10_b4_re_f
7_12_f3_99_a2_ee_9d_1e_91_35_91_1e_77_12_47_0b_2d_ec_54_53_4c_a3_8c_f7_09_47_42_47_b3_a9_70_07_3e_
52_e7_6d_e7
15:01:147.169748 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap 0="snmptrap" [Encrypted PDU]f1_
8e_0d_4c_c3_19_9a_8d_e0_e0_f8_50_8a_83_eb_70_29_65_c2_be_4d_46_8e_a1_2f_58_b2_63_72_62_0d_10_9a_3f_
37_88_e1_fa_21_cf_05_77_e4_52_03_ff_08_08_37_f0_6f_23_21_86_99_2f_8e_02_04_c8_24_12_25_02_89_74_9
f_0d_8d_b1_93_1c_fa_bb_bd_43_41_b4_d3_9e_54_8d_10_a6_23_ba_c8_4c_43_ff_24_20_84_89_3c_07_63_94_a5_
ed_01_e9_2e
15:01:147.328695 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap 0="snmptrap" [Encrypted PDU]2e_
79_70_5e_4b_0d_e5_a7_15_15_32_66_03_a8_0c_70_37_25_41_13_c4_65_8c_e2_50_0f_c7_34_2e_03_4c_47_86_d1_
1c_92_b5_c4_07_1a_89_95_b0_3f_12_c2_be_5f_94_7f_2a_39_00_e2_e6_23_71_44_4b_6d_18_4c_64_0a_e8_43_c
f_d6_98_ef_45_9e_cf_4b_85_fe_16_3b_9d_16_e2_a6_d5_98_fa_72_bc_8e_39_5a_43_a3_fa_29_a1_ca_1c_c8_ad_
75_01_b3_4f_4e_9c_cc_9b_35_5b_5d_10_e5_35_0c_4f_40_9c_63_72_b9_b8_a1_4c_db_6e_4e_47_5d_re_65

```

- Make sure the **Destination** value (*Management* -> *SNMP Setup* page) is correct (otherwise, no trap is sent, as observed with tcpdump/packet capture)
- Make sure the SecureSync's **EngineID** value is correct, on both the SecureSync (*Management* -> *SNMP Setup* page) and the SNMP Manager (otherwise, no trap is sent, as observed with tcpdump/packet capture)
- Make sure **Auth** and **Priv** field values are correct (on both the SecureSync and the SNMP Manager)

## Potential/known conditions associated with SNMP/Notification

### 1) Major alarm “active”/ Minor alarm “pending” (active) SNMP Traps not being sent (only Major/Minor “clear” traps are sent)

- Refer to Salesforce case 231544
  - As tested by Keith: Observed in v5.8.6 (they are being sent in 5.8.8/5.8.9)
  - Testevent/sendtrap lists only commands for major/minor alarm “active” traps (not for “clear” traps).

```

Usage: sendtrap <evtID> [evtID] [evtID] ...
trapID: 1=Sync 2=Holdover
 3=Freq Error 4=Freq OK
 5=User Minor Alarm 6=User Minor Clear
 7=User Major Alarm 8=User Major Clear
 9=GPS Antenna 10=Minor Alarm
 11=Major Alarm 12=Reference Change
 13=1PPS Error 14=1PPS OK
 15=Hardware Error 16=Oscillator Alarm
 17=Oscillator OK 18=Reboot
 19=Minor Temp Alarm 20=Minor Temp Clear
 21=Major Temp Alarm 22=Major Temp Clear

```

- But the Major/Minor testevent/sendtrap commands send only “clear” traps (instead of “active” traps)

---

**Name:** iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncObjs.ssSystemStatusObjs.ssSysStaMajorAlarm.0  
**Value:** [Integer] clear (2)

---

- A system reboot sends only the Major/Minor “clear” traps (not the “pending” traps)

Description	Source	Time	Severity
trapOID: iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncEvents.sseventsV2.ssevtV2FrequencyError	10.10.162.238	2020-05-28 11:37...	
trapOID: iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncEvents.sseventsV2.ssevtV2MajorAlarm	10.10.162.238	2020-05-28 11:37...	
trapOID: iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncEvents.sseventsV2.ssevtV2RefChange	10.10.162.238	2020-05-28 11:37...	
trapOID: iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncEvents.sseventsV2.ssevtV2GpsAntenna	10.10.162.238	2020-05-28 11:37...	
trapOID: iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncEvents.sseventsV2.ssevtV2MinorAlarm	10.10.162.238	2020-05-28 11:37...	
trapOID: iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncEvents.sseventsV2.ssevtV2GpsAntenna	10.10.162.238	2020-05-28 11:37...	
trapOID: iso.org.dod.internet.private.enterprises.netSmp.netSmpNotificationPrefix.netSmpNotifications.notifyShutdown	10.10.162.238	2020-05-28 11:36...	

Source:	10.10.162.238	Timestamp:	20 seconds	SNMP Version:	2
Trap OID:	iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncEvents.sseventsV2.ssevtV2MajorAlarm				
Variable Bindings:					
Name:	iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0				
Value:	[TimeTicks] 20 seconds (2070)				
Name:	snmpTrapOID				
Value:	[OID] ssevtV2MajorAlarm				
Name:	iso.org.dod.internet.private.enterprises.spectracom.specProducts.specSecureSyncMIB.specSecSyncObjv2.ssevtV2GpsAntenna				
Value:	[Integer] clear (?)				

## 2) ssGPSRefTable/SNMP\_Generic\_Error

...”Our application fetches some scalar values, which return just fine, and then uses GetBulk to fetch values from the ssGpsRefTable table, with a SNMP time out value of 10000 msec. The GetBulk is returning a SNMP\_GENERIC\_ERROR status code, as seen in the following tcpdump

- Refer to Salesforce case 19122 for Hughes
- Noticed with 5.2.0. Fixed with version 5.3.0 update.

## 3) (applicable to 5.2.0 and below) User changes to SysObjectID value isn’t propagating through SNMP.

**Note:** This appears to be an issue with at least version 5.2.0 and below. Refer to Mantis 2973. Changing it doesn’t appear to be propagating all the way through SNMP (Status update, 23 Apr 15). It appears Mantis 2973 is being fixed in the version 5.2.1 update.

## 4) Issue with SNMPv3 connections after updating from earlier version to a version such as version 5.2.0

**Summary:** May not be able to connect using SNMPv3 after applying a software update. Part of the SNMPd.conf file is missing settings for V3, preventing permissions to connect.

- Eric Girard had a customer update from 5.1.4 to 5.2.0 and reported the SNMPd.conf file was missing the settings for the group permissions after updating. But the before/after web browser screenshots were identical.
- Oleg had previously noticed that the group permissions of the SNMP v3 settings weren’t being brought forward. These don’t affect the settings in the browser at all, but will prevent the ability to connect to SNMP using V3.
- Simple Fix is to reset JUST the SNMP configs and then reconfigure just SNMP as desired.

Using the button in the upper-left corner of the **Management** -> **SNMP Setup** page of the newer browser, press the “**Restore Default SNMP Configuration**” button to reset just the SNMP settings back to factory default. Then they can reconfigure these settings only, as needed for the V3 connections. After that, they should be all set!!!

## 5) General issues with SNMP/Notifications (A specific example was Notifications page configuration issues and not sending traps when it should)

- Refer to Salesforce case 16867 (for Brian Carlson).
- The newer black/charcoal browser now has a “**Restore Default SNMP Configuration button**” in the **Management** -> **SNMP Setup** page which resets just the SNMP configs (alleviating the need to perform a full clean of all configs. Not sure what rev (version 5.1.7 or before) this button was added to the newer browser.

- Brian Carlson with Harris was seeing weird issues with the configuration of the Notifications page and traps not being sent when they should. Using this button and reconfiguring SNMP fixed these peculiar issues.

---

## 6) Having more than one SNMPv1 or v2c user with the same “Community” name

- When more than one v1/V2c user is added, each must have its own unique “community name” (such as snmptest and snmptest1 for instance).

For testing, there was already a v1 user as **snmptest**. I added a v2c user with **snmptest** also. SNMP went into a weird state with the browser and cli showing conflicting info.

---

## 7) Issue with OID “ssSysStaEstPhaseError” (OID 18837.3.2.2.1.8.0) when the returned phase error value is a negative number

- This issue was fixed in update version 5.2.1 (May 2015) Is an issue with at least versions 5.2.0 and below).
- Refer to Mantis case 3005 "
- Refer to SalesForce case 17326
- Positive phase errors are fine. Negative phase errors are fine in the browser, but SNMP poll of this OID responds with an erratic value.

**Per Dave Sohn (6 March 2015) regarding version 5.2.0 software.** The MIB and SNMP agent is incorrectly calling that out that OID with syntax of Unsigned32, when it should be Integer32. This will be resolved in the next release.

---

## 8) SNMP Manager log entry “Error building ASN.1 representation (Can’t build OID for variable)

- If the unit was updated from versions 5.1.4 or below, make sure the update process was run a second time to also update the GNSS receiver to v1.07 (if RES-SMT-GG receiver is installed)
- The v5.1.7 update changes some of our API calls due to changes Trimble has added in the v1.07 upgrade. Updating the system but not the receiver breaks some of these API calls associated with comms with the receiver.

Snmpd.log just kept going:

```
fse@Spectracom-CLK1 /home/spectracom $ cat snmpd.log.rg
```

```
Created directory: /var/run/net-snmp
```

```
Created directory: /var/run/net-snmp/mib_indexes
```

```
Turning on AgentX master support.
```

```
NET-SNMP version 5.6.1
```

```
snmp_build: unknown failuresend response: Error building ASN.1 representation (Can't build OID for variable)
```

```
-- SNMPv2-SMI::enterprises.18837.3.3.1.3.0
```

```
-- SNMPv2-SMI::enterprises.18837.3.3.1.4.0
```

```
-- SNMPv2-SMI::enterprises.18837.3.3.2.1.0
```

```
-- SNMPv2-SMI::enterprises.18837.3.3.2.2.0
```

```
-- SNMPv2-SMI::enterprises.18837.3.3.2.3.0
```

```
-- ccitt.135597392.135453712.135482736.0.0.135484120.0.33.11.0
```

```
-- ccitt.135597392.135453712.135482736.0.0.135484120.0.33.11.0
```

```
snmp_build: unknown failuresend response: Error building ASN.1 representation (Can't build OID for variable)
```

```
-- ccitt.135597392.135453712.135482736.0.0.135484120.0.33.11.0
```

```
-- ccitt.135597392.135453712.135482736.0.0.135484120.0.33.11.0
```

```
snmp_build: unknown failuresend response: Error building ASN.1 representation (Can't build OID for variable)
```

```
-- SNMPv2-SMI::enterprises.18837.3.3.1.3.0
```

---

## 9) SNMP crashing/difficulty restarting SNMP. Issues with SNMP polls stopping/restarting later or being very sluggish when walking the MIBS.

**Note:** These issues will likely be fixed with the **version 5.2.0** release (Jan 2015).

**Update to note above:** v5.2.0 has also exhibited SNMPd crashes (but not SNMPSAD crashes). Oleg has applied a patch for version 5.2.1 that appears to correct this issue. Refer to Mantis case 2995.

### Summary of software changes associated with SNMP and/or SNMPSAD crashes (ascending order)

- Refer also to the SNMP Tech note (towards the end) for software changes associated with SNMP: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP>
  - 1) **Version 5.1.2:** Temporarily disabled integers 3 and 4 for NTP\_Current\_Mode object. Timeout value in SNMP Manager set too low causes SNMPSAD to crash without being automatically restarted.
  - 2) **Version 5.1.3:** Re-enabled integers 3 and 4 for NTP\_Current\_Mode object. Added ability for rexd to automatically restart SNMPSAD (not SNMPD) if SNMPSAD crashed (due to the timeout value being set too low for NTP objects).
  - 3) **Version 5.2.0:** updated Net-SNMP to a newer version (but SNMP is still intermittently crashing).
  - 4) **Version 5.2.1** (~Apr 2015) Oleg has applied a patch for version 5.2.1 that appears to correct this issue. Refer to Mantis case 2995.

### Note/Status update (based on version 5.2.0 software update)

- Refer to Salesforce Case 17233 and Mantis case 2995.

(27 Feb 2015 KW) With 5.2.0 software installed, a couple of customers have observed SNMPD crashing (snmpsad not crashing). Daniel Hagan reported the following:

  - 1) System is successfully configured on v5.1.7 with SNMPv3 polling from SolarWinds.
  - 2) System is upgraded from v5.1.7 to 5.2.0.
  - 3) Within the space of approx. 24 hours (not identical across units, at least one unit was stable for several days), SNMP stops responding.
  - 4) Logging into the NetClock and checking Management > SNMP shows that the SNMP switch is now set to Off.
  - 5) Setting SNMP to "on" results in the GUI responding that SNMP is enabled. However, polling does not function.
  - 6) Rebooting the NetClock will allow SNMP to function post-reboot.

I was able to duplicate the issue rather quickly by creating two SNMPv3 users and performing looped SNMPwalk with one v3user and a single SNMPWalk with the other v3 user.

### Info prior to version 5.2.0 update release

- Refer to Salesforce cases such as 12049 (Ultra Electronics) <https://na8.salesforce.com/500C000000UdWVVe>
- Likely walking the SNMP MIBS
- Review the daemon.log for SNMP entries. Examples below
  - [Spectracom-CLK2 /etc/init.d/snmpd\[22014\]: WARNING: snmpd has already been started](#)
  - [Spectracom-CLK2 /etc/init.d/snmpd\[22442\]: start-stop-daemon: no matching processes found](#)
- Review the kern.log log to see if there are Segfault entries showing SNMPD crashing (examples below). Note the info in the segfault entries may vary.
  - [kernel: snmpd\[3710\]: segfault at 17 ip b76ad597 sp bfc49a30 error 4 in libnetsnmpagent.so.25.0.1\[b768e000+67000\]](#)
  - [kernel snmpd\[1841\]: segfault at 17 ip b7701597 sp bfd8d740 error 4 in libnetsnmpagent.so.25.0.1\[b76e2000+67000\]:](#)
- Review the rexd.log log to see if there are entries showing SNMPSAD being reset (examples below). These

entries indicate SNMP is crashing and needing to be restarted to resume operation. (note rexd.log is in software versions 5.0.2 and higher)

```
Oct 18 14:17:01 [RESTART] Restarting initiated for snmpsad
Oct 18 14:17:08 [SUCCESS] Successfully restarted snmpsad
```

```
Oct 18 16:46:25 [RESTART] Restarting initiated for snmpsad
Oct 18 16:46:32 [SUCCESS] Successfully restarted snmpsad
```

## Follow-up to this issue

### SNMPSAD (SNMP sub-agent) crashing

**(9 Jan 2014 KW)** We have since found that one particular NTP Status OID needs to take longer than all of the other OIDs to fully respond. The SNMP Manager is not waiting long enough for it to receive the response from the SecureSync before it's moving on to the next OID in the walk. But the response to the previous query is still waiting inside the SecureSync to be sent, even though the SNMP Manager has already moved ahead to the next OID. This causes the data to be sent to a buffer, and continuously walking the MIB causes the buffer to continue to fill.

The solution is to give the SNMP Manager a little extra time to receive the response to this "NTP" OID. A 10 second timeout is marginal. Sometimes it will provide enough time and others, it misses it. Our Engineers recommend using a timeout value of 20 seconds to be safe. Since changing this timeout, we are no longer seeing this same condition here.

**Note:** Not all SNMP Managers have the ability to change the timeout value. Oleg said the freeware programs seem to be hard-set at 5 seconds, which isn't long enough to handle this.

### SNMPd (SNMP agent) crashing/difficulty restarting (versions 5.2.0 and below)

- Daemon log entries such as:

```
WARNING: snmpd has already been started
snmpd[10061]: start-stop-daemon: no matching processes found
```

We googled the "segfault" entries associated with SNMP in a couple of kernel logs which indicated that walking the SNMP MIBs in earlier versions of the SNMP package (like the SNMP version installed in all versions 5.1.7 and below) can cause these crash errors to occur. It's highly recommended that all customers walking the mibs or performing lots of SNMP gets update to versions 5.2.0 or above (5.1.7 helped, but v5.2.0 is updating NET-SNMP to a much newer version which should help even more).

---

### Cron log reports "[RESTART] Restarting initiated for snmpsad" followed by "[SUCCESS] Successfully restarted snmpsad"

These two log entries are an indication that only the SNMPSAD subagent was restarted – not the SNMPd agent being restarted because our "watchdog" detected snmpsad wasn't running.

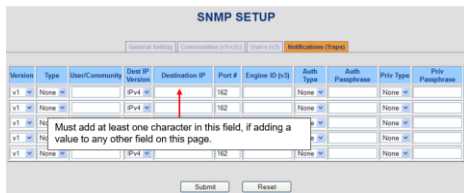
If snmpsad crashes and needs to be reset, non-spectracom mibs will still be fine, but the spectracom mibs won't be able to respond until snmpsad has successfully restarted.

snmpsad is being updated in software version 5.2.0 to allow SNMP to be updated to a newer version. If these two entries are periodically being asserted, it's recommended to update to at least version 5.2.0.

---

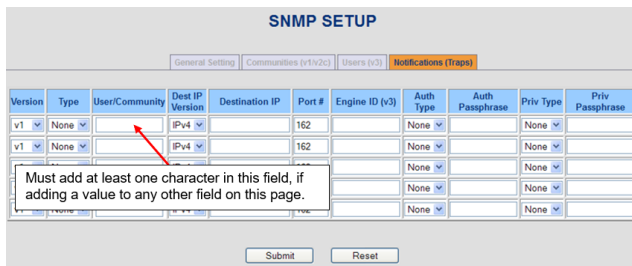
### SNMP in Archive versions 5.0.1 and 5.02 and below (web browser becomes inaccessible after leaving the "Destination IP" field blank and then pressing Submit).

- Error message occurs while configuring SNMP, if the Trap Destination IP field is left null before pressing Submit. Can't access the web browser afterwards.



**SNMP in Archive versions 4.7.0 and below (web browser becomes inaccessible after leaving the “User/Community” field in the Notifications tab blank and then pressing Submit)**

- Note: this issue was fixed in version 4.8.0



**Error message occurs while configuring SNMP. Can’t access the web browser afterwards.**

ERROR: The web server encountered an unexpected error and failed to display the page you required. It is possible, some defects exist in the web page. We will appreciate if you could kindly contact us to let us know the problem. We will investigate and fix the problem as soon as possible to ensure the quality of our product."

Perform a clean command from Setup port to restore connectivity. Refer to Mantis case 1477 and “Todd Belcher” in Salesforce. **Note:** An automatic reboot occurs when performing a clean command.

The email below described what causes this to happen and how to prevent it from happening again. I have some new information for you, regarding the lock-out condition the SecureSync was exhibiting when you were configuring its SNMP. We have figured out what is allowing this to happen and so we can now tell you how to avoid it occurring!

In the **Network / SNMP Setup** page of the browser, “**Notifications**” tab, the **User/Community** field is a required field. If this field is empty (while other values have been entered in the same row) when you hit Submit, the empty field affects the web browser operation and will lock you out, like you have been observing. As long as there is something entered in this (preferably the correct value for your SNMP manager, but any character will work) and you hit Submit, you will no longer experience this lock-out condition.logs

We were only able to duplicate the symptoms, when this one field was empty and the Submit button was pressed. Because it’s a required field for generating SNMP traps, we intend on modifying the software in a future release so that it ensures that the field is not empty, when editing the SNMP trap configurations.

Just thought you would like to know how to prevent the lock-out condition from occurring. I still have you record flagged in our Customer Service database to let you know when the software has been modified to check for a value in this field before accepting the changes.

**SNMP Returns “no Such Object” (change to the SecureSync MIB file between 4.4.0 and 4.6.0)**

- Refer to Curtis Somers, Salesforce case 12049



**SNMP still returns “no such object” but can recover from the error now. Results are randomly:**

- All OID results OK
- Only OID 1.3.6.1.4.1.18837... says “no such object” but 1.3.6.1.2.1.1.6.0 is OK
- Only one OID 1.3.6.1.4.1.18837.3.3.2.1.0 says “no such object” and all others are good

**Result** I really want to see you get this SNMP issue resolved!! So I just went back towards the beginning of the email chain and spent some time playing with SNMP Gets. I wasn't using any scripts. I was just initially performing a walk and then individually getting the value you've reported as “No Such Object”. This OID was responding just fine for me.

After thinking about this for a few moments, I recalled there had been a very minor change to one of the MIB files back a few Archive software versions ago. So I started comparing the “ssSysStaSyncState” OID in each of the “Spectracom-SecureSync-Sync.MIB” files for each version of Archive software, and found this OID had been slightly modified.

Can you do me a favor and search your Spectracom-SecureSync-Sync.MIB file for “**ssSysStaSyncState**”. If you have the newer iteration of this file, it should look like the following:

```
frq Frequency reference (i.e. frq0, frq1, etc.)
hst Host system reference (i.e. hst0, hst1, etc.)
self Internal reference"
 ::= { ssSystemStatusObjs 4 }

ssSysStaSyncState OBJECT-TYPE
SYNTAX INTEGER { sync(1),
 nosync(2) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Status of the unit's synchronization with its time/lpps
references."
 ::= { ssSystemStatusObjs 5 }

ssSysStaHoldoverState OBJECT-TYPE
SYNTAX INTEGER { holdover(0),
 sync(1),
 nosync(2) }
```

However, if you have the earlier iteration of this file, it will look like the following, instead:

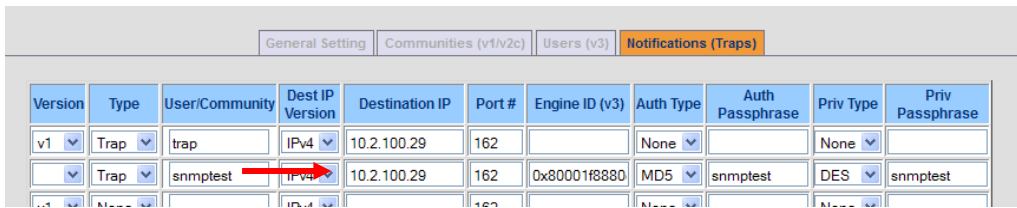
```
signal."
 ::= { ssSystemStatusObjs 4 }

ssSysStaSyncState OBJECT-TYPE
SYNTAX INTEGER { nosync(0),
 sync(1) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Status of the unit's synchronization with its time/lpps
references."
 ::= { ssSystemStatusObjs 5 }
```

Notice the integer numbers for “nosync” and “sync” have been changed. If you have the earlier iteration of this file, and the SecureSync is not in sync, the integer will respond with a 2, which is a not a valid response with this earlier MIB file. Updating to the newer version of this file SHOULD fix this for you, as far as I can see!!

If you have the earlier iteration of the MIB file, there are two ways to obtain it. The attached document discusses how to FTP/SCP transfer it out of the SecureSync. Or for your convenience, I have attached it for you. Uninstall the earlier from the Manager and install the latest,. Recompile the MIBs and I highly BELIEVE you will finally be all set.

(Network -> SNMP page, Notifications tab) SNMP "Version" field displays a Null" when SNMPv3 is selected  
➤ (Reference Mantis case 1909) at least versions 4.8.7 and below.



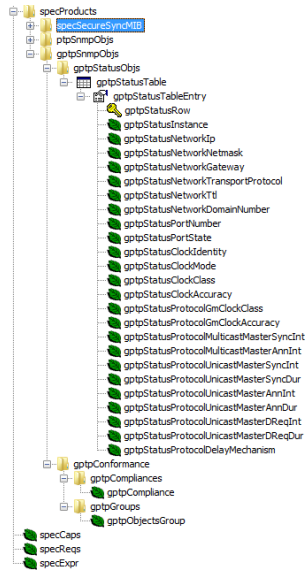
Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
v1	Trap	trap	IPv4	10.2.100.29	162		None		None	
	Trap	snmptest	IPv4	10.2.100.29	162	0x80001f8880	MD5	snmpstest	DES	snmpstest
v1	Trap		IPv4		162		None		None	

## Examples of available SNMP Gets/Sets

### PTP mib file (for 1204-12 10/100 card) and GB PTP mib file (for 1204-32 card)

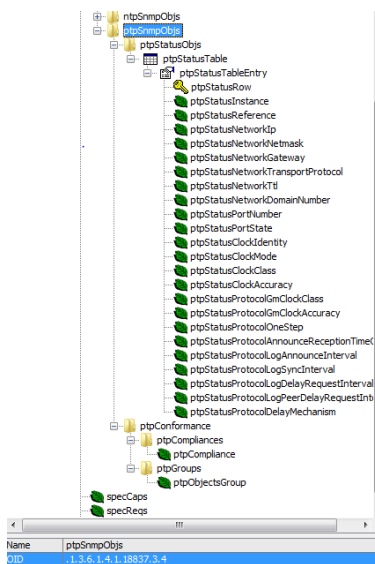
#### A) “SPECTRACOM-GPTP.mib” file/objects (starts with .1.3.6.1.4.1.18837.3.5)

- This much more recent PTP mib file was added in software version 5.6.0 (Apr 2017) for the 1204-32 (Gb PTP Option Card)
- All of the object names begin with “gptp” (such as **gptp**StatusTable” for instance)



#### B) SPECTRACOM-PTP-MIB.mib” file/objects (starts with .1.3.6.1.4.1.18837.3.4)

- This much earlier PTP mib file is for the Model 1204-12 (10/100 PTP Option Card)
- All of the object names begin with “ptp” (such as ptpStatusTable” for instance)



C) Note: Using the PTP Mib (10/100) file with a Gb 32 card (instead of using the GB Mib) results in the responses returning values such as “no Such Instance” or all “zeroes”.

ptpStatusNetworkIp	No Such Instance	NoSuchInst...	10.2.
ptpStatusRow	(Snm No Such Object)	NoSuchObject	10.2.
ptpStatusInstance	No Such Instance	NoSuchInst...	10.2.
ptpStatusReference	No Such Instance	NoSuchInst...	10.2.
ptpStatusNetworkIp	No Such Instance	NoSuchInst...	10.2.
ptpStatusNetworkNetmask	No Such Instance	NoSuchInst...	10.2.

## SNMP Gets available via RFC1213 MIB file

### 1) Ethernet port states via SNMPGets

- Refer also to the **portstate** CLI command in the CLI section of this document.

Note that in addition to the port states being available via the **portstate** CLI command, they are also available via SNMPGets in the generic (not Spectracom-specific) RFC-1213 MIB. The name of the object for the states of each port in the RFC1213 MIB is **ifOperStatus** (as shown below):

- The ifDescr object lists all of the available interfaces in the time server and reports the “assigned name” for each one.

Object Name	Value
#Descr.1	lo
#Descr.2	tun0
#Descr.3	eth0
#Descr.4	ipb0
#Descr.5	eth1
#Descr.6	eth2
#Descr.7	eth3
#Descr.8	eth4
#OperStatus.1	up(1)
#OperStatus.2	down(2)
#OperStatus.3	down(2)
#OperStatus.4	down(2)
#OperStatus.5	up(1)
#OperStatus.6	down(2)
#OperStatus.7	down(2)
#OperStatus.8	down(2)

Note: using the

### 2) Configuring the Reference Priority table using SNMP Sets

Questions for Spectracom:

1. Do you expect the snmpset commands to work for the above referenced OIDs?
2. If not, why, and is there some other MIB/OID info you can provide to allow a time reference change via SNMP? SNMP is preferred because our data processor already has an SNMP interface for the PTU coded.
3. If SNMP set is not an option for this, what options other than the web GUI interface are available for doing this reference switch?

**Keith's response:** Section 7 (page 24) of the attached SNMP tech note discusses how to configure/reconfigure the input reference priority table using SNMP. This info is excerpted below in blue for your reference (Please especially pay particular notice to the “Note” below and in the document)

(FYI also attached is a spreadsheet I have also created which contains the more commonly used OIDs in one tab and the available SNMP traps in another tab. I hope you and your team find both the SNMP document and the spreadsheet helpful, as I suspect you will ☺!)

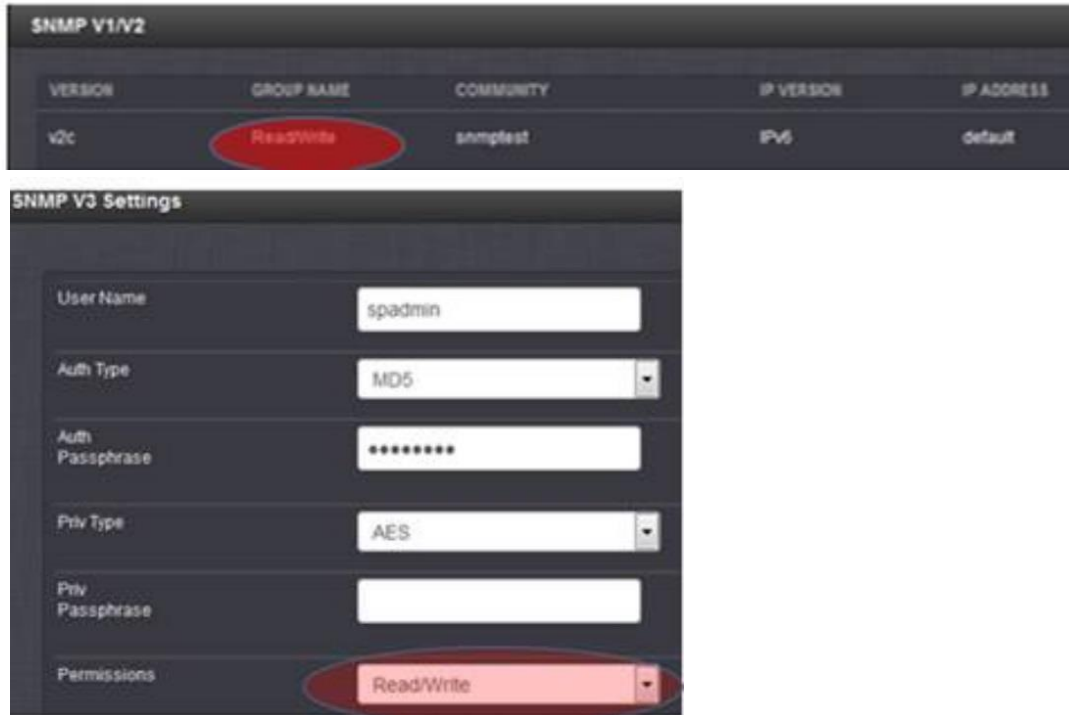
The “Enable/Disable” and “Priority” fields of the “Reference Priority Setup” can be configured via the SecureSync’s web browser or with SNMP “Sets”. The “SPECTRACOM-SECURE-SYNC-MIB.mib” file contains the applicable values for configuring this table via SNMP. Refer to “**ssReferenceMgmtObjs Objects [enterprises.18837.3.2.2.4.x]**” in this MIB file for a list of all of the values associated with this table. Refer to the SecureSync user manual for additional information on the “Reference Priority Setup” table.

**Note:** SNMP provides the ability to “get” the entire Reference Priority table, but only provides the ability to “set” the “State” field (Enable or Disable input references) and the “Priority” of the reference. SNMP does not allow entries to be

added or deleted from the Reference Priority table.

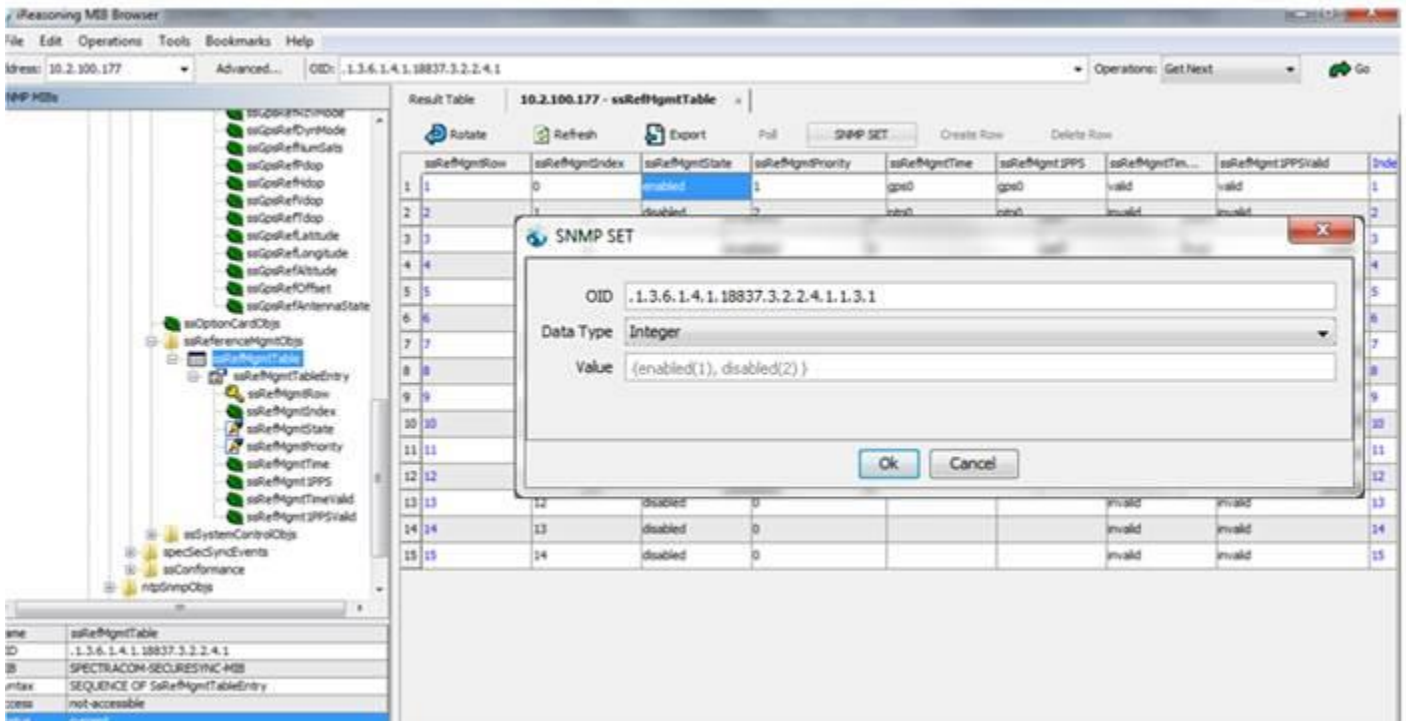
Per the “Note” above, the SecureSync’s input reference priority table should initially be pre-configured (using the **Management -> Reference Priority** page of the web browser) with a “list” of all input references that the SecureSync could potentially be synced with. Thereafter, SNMP can then be used to change the priority assigned and/or enable/disable each of the references in this table.

[With read/write privileges enabled in both the SecureSync (**Management -> SNMP Setup** page of the browser as shown below) and in the SNMP Manager]:



In the SNMP Manager’s “Table view” (as shown below), the columns of “**ssRefMgmtState**” and “**ssRefMgmtPriority**”, **the SNMP set button** allows the applicable enable/disable for each reference, and its assigned priority value (the lower the number, the higher its order of precedence for selection). After pressing the SNMP Set button, the value can be defined as either a 1 to enable or 2 to disable

**To enable/Disable each row of the table**



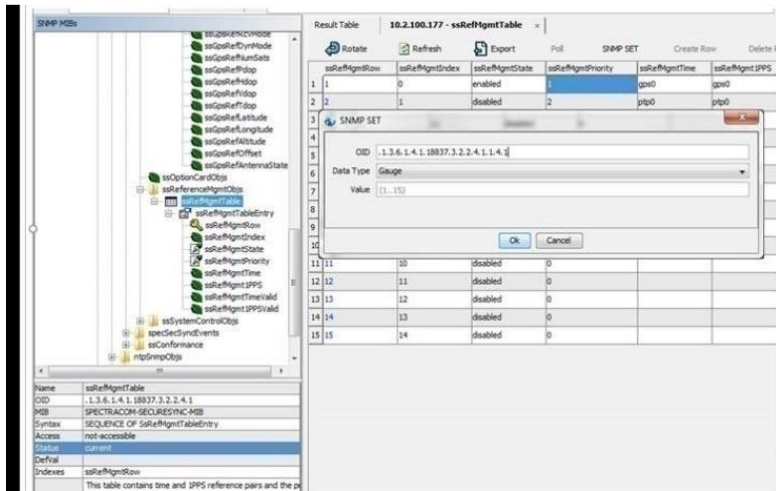
Below are the specific OIDs to enable/disable each reference.

Index (row of table)

- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.1
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.2
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.3
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.4
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.5
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.6
- etc

Note that in order to disable each reference, the value of “2” needs to be sent.

**To Change the priority of each row of the table**



Below are the specific OIDs to change the priority of each reference (available values are 1 through 15)

Index (row of table)

- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.1
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.2
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.3
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.4
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.5
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.6
- etc

## System Memory, CPU and disk usage (CF card) information via the “.2021” (UCD/UCDavis) MIB file

- Per the SecureSync release notes, ability to poll the diskstats , CPU and memory was added in version 5.2.1
  - Added ability to pull system **memory**, **CPU**, and CF card **disk usage** information from **SNMP**
  -

**Note:** These system MIBs are only available with SecureSync software **versions 5.2.1** and higher installed

### UCD/UC Davis MIB file (“UCD-SNMP-MIB”) “.1.3.6.1.4.1.2021.”

- The “.2021” MIB OIDs (such as the ones listed below) are all part of the UCD-SNMP-MIB (ucdavis) MIB file. For more information on this MIB file, which is internally supported by SecureSync, refer to: <http://www.net-snmp.org/docs/mibs/ucdavis.html>

TABLE 1: CPU USAGE	
OID	FUNCTION
.1.3.6.1.4.1.2021.11.9.0	Percentage of user CPU time
.1.3.6.1.4.1.2021.11.50.0	Raw user CPU time
.1.3.6.1.4.1.2021.11.10.0	Percentages of system CPU time
.1.3.6.1.4.1.2021.11.52.0	Raw system CPU time
.1.3.6.1.4.1.2021.11.11.0	Percentages of idle CPU time
.1.3.6.1.4.1.2021.11.53.0	raw idle CPU time
.1.3.6.1.4.1.2021.11.51.0	raw nice CPU time

TABLE 2: MEMORY USAGE	
OID	FUNCTION
.1.3.6.1.4.1.2021.4.3.0	Total Swap Size
.1.3.6.1.4.1.2021.4.4.0	Available Swap Space
.1.3.6.1.4.1.2021.4.5.0	Total RAM in machine
.1.3.6.1.4.1.2021.4.6.0	Total RAM used
.1.3.6.1.4.1.2021.4.11.0	Total RAM Free
.1.3.6.1.4.1.2021.4.13.0	Total RAM Shared
.1.3.6.1.4.1.2021.4.14.0	Total RAM Buffered
.1.3.6.1.4.1.2021.4.15.0	Total Cached Memory

TABLE 3: DISK USAGE	
OID	FUNCTION
.1.3.6.1.4.1.2021.9.1.2.1	Path where the disk is mounted
.1.3.6.1.4.1.2021.9.1.3.1	Path of the device for the partition
.1.3.6.1.4.1.2021.9.1.6.1	Total size of the disk/partition (kBytes)
.1.3.6.1.4.1.2021.9.1.7.1	Available space on the disk
.1.3.6.1.4.1.2021.9.1.8.1	Used space on the disk
.1.3.6.1.4.1.2021.9.1.9.1	Percentage of space used on disk
.1.3.6.1.4.1.2021.9.1.10.1	Percentage of inodes used on disk

### Disk usage

- versions prior to version 5.2.1 did not support the **.1.3.6.1.4.1.2021.9.1.7.x** objects to poll disks status

**Problem: Unable to obtain the disk stats (such as .1.3.6.1.4.1.2021.9.1.7.1) while everything else is returned succusfully (software version well above v5.2.1)**

- Refer to Salesforce case 127293



- this was caused by a customer restoring an earlier configuration bundle into a newer version of software. As shown in the snmpd.conf file comparison below, the “Miscellaneous” section of the customer’s snmpd.conf file was missing the “diskio” comments that we had present in our snmpd.conf file (as shown below)

FYI- I ran a diff on their snmpd.conf (left side) and our Netclock 9483 (right side)

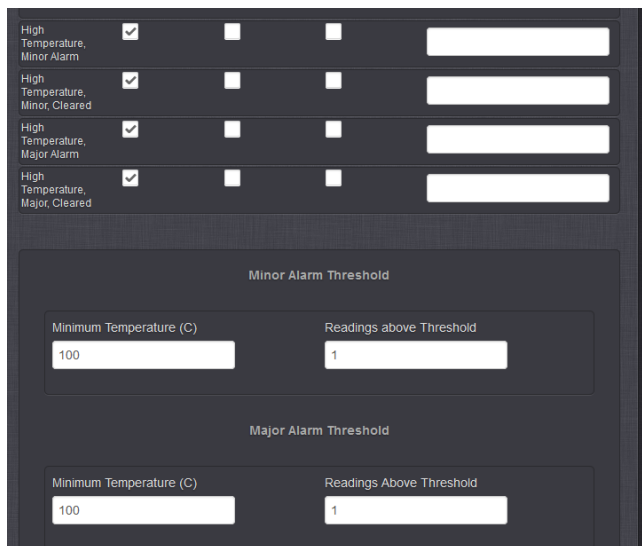
Under **miscellaneous** (at the bottom) our unit has diskIO info, while their unit doesn’t?? I think this is key, but not sure why their config would be different. Could this somehow be due to their “roprivgroup” being “**none**” and ours being “**one**”?

C:\Temp\weig\home\spectracom\config\snmpd.conf	C:\Temp\our unit\snmpd.conf
#com2sec sec.name source community	#com2sec sec.name source community
com2sec6 comuser_1 default public	
com2sec comuser_1 default public	com2sec comuser_1 default public
#group groupname sec.model sec.name	#group group name sec.model sec.name
group ronoauthgroup v1 comuser_1	group ronoauthgroup v1 comuser_1
group roprivgroup usm masnmp	group rwprivgroup usm test1234
#view name incl/excl subtree mask	#view name incl/excl subtree mask
view all included .1	view all included .1
#access name context sec.model sec.level prefix read	#access name context sec.name sec.model sec.level pr
access ronoauthgroup "" any noauth exact all none no	access ronoauthgroup "" any noauth exact all none no
access rwnoauthgroup "" any noauth exact all all none	access rwnoauthgroup "" any noauth exact all all none
access roauthgroup "" any auth exact all none none	access roauthgroup "" any auth exact all none none
access rwaauthgroup "" any auth exact all all none	access rwaauthgroup "" any auth exact all all none
access roprivgroup "" any priv exact all none none	access roprivgroup "" any priv exact all none one
access rwprivgroup "" any priv exact all all none	access rwprivgroup "" any priv exact all all none
#createUser username [MD5 SHA] [passphrase] [DES] [p	#name context sec.model sec.level prefix read write
createUser masnmp MD5 9Chuc7aZaCh9 DES 9Chuc7aZaCh9	
#trapsess [SNMPCMD_ARGS] host	#createUser username [MD5 SHA] [passphrase] [DES] [p

C:\Temp\weig\home\spectracom\config\snmpd.conf	C:\Temp\our unit\snmpd.conf
trapsess -v 2c -c spectracom udp:10.201.1.81:162	createUser test1234 MD5 test1234 AES test1234
#agentX configuration	#trapsess [SNMPCMD_ARGS] host
master agentx	trapsess -v 3 -e 0x80001f8880fa41937b7 -u test1234 -
agentXPerms 770 770 spui root	agentXPerms 770 770 spui root
agentXSocket tcp:localhost:705	agentXSocket tcp:localhost:705
agentXTimeout 5	agentXTimeout 5 # This is the def
agentXRetries 5 # This is the default	agentXRetries 5 # This is the def
#system group	# System Group
sysObjectID 1.3.6.1.4.1.18837	sysObjectID 1.3.6.1.4.1.18837.3.3.2
sysContact techsupport@spectracomcorp.com	sysContact techsupport@spectracom.com
sysLocation Unknown	sysLocation Unknown
sysDescr Spectracom Product	sysDescr Spectracom NetClock 9483
sysServices 72	sysServices 72
#miscellaneous	# Miscellaneous
agentgroup root	agentgroup root
agentuser spui	agentuser spui
authtrapenable 2	authtrapenable 1
	proc snmpd 1 1
	disk / 10%
	diskio_exclude_fd yes
	diskio_exclude_loop yes
	diskio_exclude_ram yes

## Temperature related notifications (added in version 5.3.1)

- Version 5.3.1 also added SNMP alerts for high temperatures ([Management](#) -> [Notifications](#) page, System tab)



High Temperature, Minor Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
High Temperature, Minor, Cleared	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
High Temperature, Major Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
High Temperature, Major, Cleared	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>

Minor Alarm Threshold

Minimum Temperature (C)	Readings above Threshold
<input type="text" value="100"/>	<input type="text" value="1"/>

Major Alarm Threshold

Minimum Temperature (C)	Readings Above Threshold
<input type="text" value="100"/>	<input type="text" value="1"/>

The alarms are similar in behavior to the GPS Number of Satellite Major and Minor alarms. In this case the user can set a Minimum Temperature Threshold value for both the Major and Minor alarms. The user can also set a number of times the value above the threshold must be present before asserting the Major or Minor Alarm. A value of 1 means that the value was read once, a minute passed and on reading the value again, the temperature exceeded the threshold. The number of reads is user settable to allow for environmental conditions where more than 1 read is required to validate accurate temperature. Increasing the value requires N multiple consecutive reads of temperature above the minimum threshold before asserting the alarm.

### Largest acceptable value for both Minimum temperature values is “100” (in at least versions 5.4.1 and below)

- Max value that should be entered in either temperature field is “100” (though in at least versions 5.4.1 and below, the browser will accept a value greater than 100 with no error messages being displayed).
- Setting either or both of the “Minimum temperature” fields to a value greater than “100” will cause statusd daemon to keep restarting (as indicated in the system.log. NTP will still be able to run, but NTP status info (stratum, sync status, etc.) will be reported as “?” because statusd will keep clearing out the values obtained from NTPQ.

---

## Notifications/traps for SAASM receiver only

- Refer to SecureSync SAASM receiver Manual Addendum (1200-5000-0053)
  - **Note:** NOT in Arena, as it’s an FOUO document: [\\rocuso.uso.oroliausa.com\us-only\Documentation\Released\Manuals\1200-xxxx-xxxx](http://rocuso.uso.oroliausa.com/us-only/Documentation/Released/Manuals/1200-xxxx-xxxx)
- There are no Minor/Major alarms associated with SAASM receivers (key status has no effect on the Fault LED)
- There are a few specific EMAIL notifications available for just SAASM receivers (as of at least version 5.3.0, Sept 2015, there are no SNMP traps or OIDs associated with these email alerts).
- These specific email notifications (key expiration) are only displayed in web browser if a SAASM receiver is installed.
- I submitted Mantis case 3213 (Jan 2016) as an enhancement to add OIDs associated with the SAASM receivers.

### Known issues with Notifications for SAASM receivers (Oct 2015)

- Refer to Mantis case 3145
- With at least v5.3.0 (and not sure how far back), when a SAASM receiver is installed, the email notification

configurations are not displayed in the new web browser (though they are in the classic interface) as they should be. Users will need to configure them in the classic interface browser, if they wish to enable them.

---

## Testing SNMP traps and email alerts

- Refer to (in this document): [\\*\\*Testing/Verifying SNMP/Email alerts are enabled and working](#)

---

## Known SecureSync issues

- **Version 4.2.0 software** (Refer to NC 4311 in NC database). Seven orders shipped with this version installed. Units w/4.2.0 that are either cleaned at the factory or are upgraded to 4.2.0 in the field and then cleaned by the customer will not retain their static values upon a power cycle. Orders shipped with or notified about v4.2.0 update should be limited to T-31895, T-32084, T-32382, T-32529, T-32229.
- **Versions prior to version 4.2.1-** "spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)" log entries may be continuously asserted into the equipment. This is a KTS version issue: Per Mike Sander: "They are running NWP 4.1.0 SW and KTS 2.0.0. They should have KTS 2.1.0. Upgrading to 4.2.1 will fix the problem".

This will happen if you send a new CF card that upgrades the main but not the other versions of software not installed on the card. Supposedly (verify with Engineering) the cards contain all of the updates, but if the customer performs an update? (which updates all software modules) they will be ok (this concept just prevents them from having to download all of the files from the site).

- Rubidium oscillator SecureSyncs with versions prior to version 4.3.2. Version 4.3.1 resolve some and Version 4.3.2 resolves the remaining following issues in Rb-based appliances:
- Intermittent Frequency Error alarms in Alarms log.
- Large phase errors reported in the Time and Frequency Status screen.
- Oscillator maintenance alarms associated with the Rb oscillator.

Approximate version 4.3.2 cut-in date is about Nov 12, 2010.

- Versions 4.3.2 and below will show great NTP jitter an offset values inside the box. However, clients syncing to the SecureSync will see excessive NTP jitter from SecureSync (upwards of the tens of milliseconds, such as 50-60 milliseconds, or even higher).
- Updating from an earlier version to version 4.5.0 (4.5.0 was released to MFG, but not made available on the website) due to new Osc log., some of the Facility and Severity code configs cause the logs to "inter-twine" themselves. V4.5.1 to likely resolve this issue.
- At least Version 4.5.0 and below, may potentially see "ghost Option Cards" temporarily "installed" in Option Bays, when the bay is actually empty. A power cycle clears this false indicate.
- Can't field-update any of the Model 1204-12 PTP Option Cards that were running on version 4.4.0 software. The PTP module (or the whole unit) needs to be returned to factory to apply any updates to the board beyond 4.4.0 (as far as I am aware, this should be limited to Morgan Stanley -Will Hickey and JT3- Leisa Butler).
- LCD goes blank almost immediately after issuing a "Halt" command (instead of displaying the system is shutting down and power off).

Refer to Salesforce case 00003917 for details. Can be caused by one of the ETX BIOS values being set incorrectly:

One of the settings in the "PnP/PCI Configuration" menu ("Power Management") of the BIOS has a choice of either "Disabled" or "ACPI". We select "Disabled" in order to prevent the micro from removing power, so that the shutdown splash screen can continue to be displayed. If it was inadvertently selected as "ACPI" at the factory, the splash-screen would be momentarily displayed and then would no longer be visible.

- Error message occurs while configuring SNMP. Can't access the web browser afterwards.

ERROR: The web server encountered an unexpected error and failed to display the page you required. It is possible, some defects exist in the web page. We will appreciate if you could kindly contact us to let us know the problem. We will investigate and fix the problem as soon as possible to ensure the quality of our product."

Perform a clean command from Setup port to restore connectivity. Refer to Mantis case 1477 and Todd Belcher in Salesforce. Note: An automatic reboot occurs when performing a clean command.

**Note:** this issue was fixed in software version 4.8.0

**Email sent to In-Sup Lee (4/24/12 = Refer to case 5345)** As for the web browser error message they reported, what was your customer doing in the web browser, just prior to this error being displayed? Were they configuring SNMP/Email notifications? What is the current Archive software version in the SecureSync (as reported in the Tools -> Versions page of the web browser)?

If the error is still being displayed, preventing them from being able to access the web browser, I recommend they reset the NTP server back to the factory default settings. Then, they can configure it as desired. If the software version is prior to version 4.8.0, either have them update the software to version 4.8.5 software, or at a minimum if they are configuring SNMP, have them add any character (such as a "C", for instance) or any number (such as a "1") into the "**User/Community**" field on the Network -> SNMP Setup page of the browser, "Notifications" tab. This is to prevent this particular field from being blank when the Submit button is pressed. Otherwise, this error message can be displayed. The version 4.8.0 software update prevents this issue from occurring.

To clear the error message and to restore operation, perform a "clean" CLI command to reset the logs and configs back to factory default values. A "clean" command can be performed by connecting a PC running HyperTerminal (or other terminal emulator software) to the front panel SERIAL port with a straight-thru DB8F to DB9F serial cable. The settings for HyperTerminal are 9600, N, 8 1. Once connected, type: clean <enter>. Note that this same command can also be sent with a telnet or an SSH connection (as long as these services are still enabled in the web browser). Either telnet or ssh into the NTP server and then type: clean <enter>. After issuing this command via RS-232, telnet or SSH, the logs and configurations will be reset and the web browser should be accessible again. Then just configure the SecureSync as desired.

### **Temporary fix to this SNMP lock-out condition**

I have some new information for you, regarding the lock-out condition the SecureSync was exhibiting when you were configuring its SNMP. We have figured out what is allowing this to happen and so we can now tell you how to avoid it occurring!

In the **Network / SNMP Setup** page of the browser, "**Notifications**" tab, the **User/Community** field is a required field. If this field is empty (while other values have been entered in the same row) when you hit Submit, the empty field affects the web browser operation and will lock you out, like you have been observing. As long as there is something entered in this (preferably the correct value for your SNMP manager, but any character will work) and you hit Submit, you will no longer experience this lock-out condition.

We were only able to duplicate the symptoms, when this one field was empty and the Submit button was pressed. Because it's a required field for generating SNMP traps, we intend on modifying the software in a future release so that it ensures that the field is not empty, when editing the SNMP trap configurations.

Just thought you would like to know how to prevent the lock-out condition from occurring. I still have you record flagged in our Customer Service database to let you know when the software has been modified to check for a value in this field before accepting the changes.

- Sluggish operation with a Gigabit Card (1204-06) installed (Refer to ECN 2800)

**(12/6/11 KW Email I sent to Sylvain)** The issue may be due to two wrong components soldered onto the Gigabit Option Card (installed in a rear panel Option Bay). There was an earlier part replacement on this Option Card that we recently learned was inadvertently switched back to the earlier parts, in a newer version of the Bill of Materials. This wrong part being installed can cause the symptoms that were reported (very sluggish operation).

There are two locations on the Gigabit card that are labeled for a capacitor to be installed (C245 and C246). These were later changed to be a 0 ohm resistor installed in place of the two original capacitors that were installed in these two locations. The BOM was changed for a different reason altogether, but during this change, these two parts were incorrectly changed back to capacitors again. Please take a look at these two locations and determine if a resistor was installed, or as we suspect may likely be the case, a capacitor is instead installed in these two locations, instead.

Just by removing the Gigabit Option Card from the SecureSync will likely cause the unit to operate normally again. This will confirm the issue is with this card. If these two locations have a capacitor installed, replacing the two caps with two 0 ohm resistors and then reinstalling the Option Card will likely resolve this issue!!!

ECN 2800 Changes C245 and C246 to 0 ohm resistors.

- (12/14/11 KW): Reported by Kris Fear--Refer to Mantis case 1577 for more details) Versions 4.7.0 and below.

Local clocks assigned to one particular output can also affect other outputs, as well (related to having multiple Option Cards with multiple instances)

- (5/31/12 KW) LCD window keeps scrolling through data, even though nobody is touching the keypad. We found the front panel ribbon cable is getting cut by the front panel metal, causing it to short out. Will be soon adding tape to the metal edges as a temp fix, until a permanent fix is put into place.
- Dropped packets on Gigabit Option Card (1204-06). Results in intermittent loss of all network communication. Reboot is a temporary fix. Refer to Morgan Stanley cases for more detail. A glitchy power save feature needed to be disabled with a bit in the FPGA. Fixed in 4.8.6 software update.
- PTP Option Card (1204-06) Versions 4.8.5 and below: Cards respond to ping just fine from Windows PCs but not from Linux machines. Fixed in 4.8.6 update.
- GPS Survey is restarted in Standard mode after each reboot (noticed w/4.8.6 installed).

Refer to Mantis case 1734 for more info.

**Email from Dave Lorah to internal/engineering**

In today's 2:00 conference call with Hughes Network Systems I will tell them the problem turned out to be a software bug that occurs if switching to Mobile Mode after the GPS Survey is completed. Doing this corrupts the config files. This results in the unit sometimes restarting the survey after a power cycle.

There is a workaround where a Clean/Halt can be performed and this will solve the problem. But if placed in Mobile Mode after the survey is completed it will have the problem again.

Paul said this can be fixed for the next firmware release due in Sept/Oct.

**Email from Dave Lorah to Hughes (7/13/12)**

As we discussed yesterday, the problem with the SecureSync restarting the GPS Survey after a power cycle is caused by a corruption of the configuration files. The files can become corrupted if the GPS Mode is changed from the default setting "Standard" mode to "Mobile" mode after the initial survey has been completed.

We are working on a correction for this and it should be included in the next scheduled firmware release. The release is scheduled for Sept/Oct 2012.

In the mean time we have a workaround to prevent the error from occurring and to correct any corrupted configuration files.

If the problem exists there is a way to clear the error from the config files in the SecureSync. By performing a CLEAN/HALT function from the web browser the configuration files are cleared out and any erroneous files erased. This sets the unit to factory defaults.

Then you must avoid manually changing the GPS Mode to "Mobile" mode. You should not have to do this anyway. Just leave the unit at defaults and it will operate automatically.

**To perform a CLEAN/HALT function:**

- Open the web browser for the SecureSync unit
- Navigate to the TOOLS/UPGRADE/BACKUP screen
- Select the CONFIGURATION tab
- Change the Clean/Halt field from Disabled to Enabled and select SUBMIT
- This will clear out the configuration files and any erroneous settings. The unit will HALT operation and will need a power cycle to resume operation.

**Issue with erratic System log entries in units with Rb oscillator installed**

➤ (Refer to Mantis Case 1729)

Applicable in at **least version 4.8.6** software (Likely to be fixed in the next release).

Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL\_Get - Label(oscillator\_ca\_dac0) - devindex(0) - index(4294967295) (WEB)

Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true XO\_GetDac 0 (KTSAL)

Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR

---

## Known SecureSync issues

- 1) Can't enable certain subnet masks (such as 255.255.255.192) via the front panel interface (configuring via the web browser is fine). Mark Goodlein is aware this is an issue in version 4.0.0, but not sure if he will have time to add to 4.1.0. This will likely get fixed in version 4.2.0 release instead. Reported by Sam Simione from ontech.
- 2) Version 4.2.0 software (Refer to NC 4311 in NC database). Seven orders shipped with this version installed. Units w/4.2.0 that are either cleaned at the factory or are upgraded to 4.2.0 in the field and then cleaned by the customer will not retain their static values upon a power cycle. Orders shipped with or notified about v4.2.0 update should be limited to T-31895, T-32084, T-32382, T-32529, T-32229.
- 3) Versions prior to version 4.2.1- "spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)" log entries may be continuously asserted into the equipment. This is a KTS version issue: Per Mike Sander: "They are running NWP 4.1.0 SW and KTS 2.0.0. They should have KTS 2.1.0. Upgrading to 4.2.1 will fix the problem".

This will happen if you send a new CF card that upgrades the main but not the other versions of software not installed on the card. Supposedly (verify with Engineering) the cards contain all of the updates, but if the customer performs an update? (which updates all software modules) they will be ok (this concept just prevents them from having to download all of the files from the site).

- 4) Rubidium oscillator SecureSyncs with versions prior to version 4.3.2. Version 4.3.1 resolve some and Version 4.3.2 resolves the remaining following issues in Rb-based appliances:
- 5) Intermittent Frequency Error alarms in Alarms log.
- 6) Large phase errors reported in the Time and Frequency Status screen.
- 7) Oscillator maintenance alarms associated with the Rb oscillator.
- 8) Versions 4.3.2 and below will show great NTP jitter an offset values inside the box. However, clients syncing to the SecureSync will see excessive NTP jitter from SecureSync (upwards of the tens of milliseconds, such as 50-60 milliseconds, or even higher).
- 9) Updating from an earlier version to version 4.5.0 (4.5.0 was released to MFG, but not made available on the website) due to new Osc log., some of the Facility and Severity code configs cause the logs to "inter-twine" themselves. V4.5.1 to likely resolve this issue.
- 10) At least Version 4.5.0 and below, may potentially see "ghost Option Cards" temporarily "installed" in Option Bays, when the bay is actually empty. A power cycle clears this false indicate.
- 11) Can't field-update any of the Model 1204-12 PTP Option Cards that were running on version 4.4.0 software. The PTP module (or the whole unit) needs to be returned to factory to apply any updates to the board beyond 4.4.0 (as far as I am aware, this should be limited to Morgan Stanley -Will Hickey and JT3-Leisa Butler).
- 12) LCD goes blank almost immediately after issuing a "Halt" command (instead of displaying the system is shutting down and power off).

Refer to Salesforce case 00003917 for the details. Can be caused by one of the ETX BIOS values being set incorrectly:

One of the settings in the "PnP/PCI Configuration" menu ("Power Management") of the BIOS has a choice of either "Disabled" or "ACPI". We select "Disabled" in order to prevent the micro from removing power, so that the shutdown splash screen can continue to be displayed. If it was inadvertently selected as "ACPI" at the factory, the splash-screen would be momentarily displayed and then would no longer be visible.

- 13) Error message occurs while configuring SNMP. Can't access the web browser afterwards.

ERROR: The web server encountered an unexpected error and failed to display the page you required. It is possible, some defects exist in the web page. We will appreciate if you could kindly contact us to let us know the problem. We will investigate and fix the problem as soon as possible to ensure the quality of our product."

Perform a clean command from Setup port to restore connectivity. Refer to Mantis case 1477 and Todd Belcher in Salesforce. Note: An automatic reboot occurs when performing a clean command.



**Note:** this issue was fixed in software version 4.8.0

**Email sent to In-Sup Lee (4/24/12) Refer to case 5345.**

As for the web browser error message they reported, what was your customer doing in the web browser, just prior to this error being displayed? Were they configuring SNMP/Email notifications? What is the current Archive software version in the SecureSync (as reported in the Tools -> Versions page of the web browser)?

If the error is still being displayed, preventing them from being able to access the web browser, I recommend they reset the NTP server back to the factory default settings. Then, they can configure it as desired. If the software version is prior to version 4.8.0, either have them update the software to version 4.8.5 software, or at a minimum if they are configuring SNMP, have them add any character (such as a "C", for instance) or any number (such as a "1") into the "**User/Community**" field on the Network -> SNMP Setup page of the browser, "Notifications" tab. This is to prevent this particular field from being blank when the Submit button is pressed. Otherwise, this error message can be displayed. The version 4.8.0 software update prevents this issue from occurring.

To clear the error message and to restore operation, perform a "clean" CLI command to reset the logs and configs back to factory default values. A "clean" command can be performed by connecting a PC running HyperTerminal (or other terminal emulator software) to the front panel SERIAL port with a straight-thru DB8F to DB9F serial cable. The settings for HyperTerminal are 9600, N, 8 1. Once connected, type: clean <enter>. Note that this same command can also be sent with a telnet or an SSH connection (as long as these services are still enabled in the web browser). Either telnet or ssh into the NTP server and then type: clean <enter>. After issuing this command via RS-232, telnet or SSH, the logs and configurations will be reset and the web browser should be accessible again. Then just configure the SecureSync as desired.

### Temporary fix to this SNMP lock-out condition

I have some new information for you, regarding the lock-out condition the SecureSync was exhibiting when you were configuring its SNMP. We have figured out what is allowing this to happen and so we can now tell you how to avoid it occurring!

In the **Network / SNMP Setup** page of the browser, "**Notifications**" tab, the **User/Community** field is a required field. If this field is empty (while other values have been entered in the same row) when you hit Submit, the empty field affects the web browser operation and will lock you out, like you have been observing. As long as there is something entered in this (preferably the correct value for your SNMP manager, but any character will work) and you hit Submit, you will no longer experience this lock-out condition.

We were only able to duplicate the symptoms, when this one field was empty and the Submit button was pressed. Because it's a required field for generating SNMP traps, we intend on modifying the software in a future release so that it ensures that the field is not empty, when editing the SNMP trap configurations.

Just thought you would like to know how to prevent the lock-out condition from occurring. I still have you record flagged in our Customer Service database to let you know when the software has been modified to check for a value in this field before accepting the changes.

#### 14) Sluggish operation with a Gigabit Card (1204-06) installed (Refer to ECN 2800)

**(12/6/11 KW Email I sent to Sylvain)** The issue may be due to two wrong components soldered onto the Gigabit Option Card (installed in a rear panel Option Bay). There was an earlier part replacement on this Option Card that we recently learned was inadvertently switched back to the earlier parts, in a newer version of the Bill of Materials. This wrong part being installed can cause the symptoms that were reported (very sluggish operation).

There are two locations on the Gigabit card that are labeled for a capacitor to be installed (C245 and C246). These were later changed to be a 0 ohm resistor installed in place of the two original capacitors that were installed in these two locations. The BOM was changed for a different reason altogether, but during this change, these two parts were incorrectly changed back to capacitors again. Please take a look at these two locations and determine if a resistor was installed, or as we suspect may likely be the case, a capacitor is instead installed in these two locations, instead.

Just by removing the Gigabit Option Card from the SecureSync will likely cause the unit to operate normally again. This will confirm the issue is with this card. If these two locations have a capacitor installed, replacing the two caps with two 0 ohm resistors and then reinstalling the Option Card will likely resolve this issue!!!

ECN 2800 Changes C245 and C246 to 0 ohm resistors.

- 15) (12/14/11 KW): Reported by Kris Fear--Refer to Mantis case 1577 for more details) Versions 4.7.0 and below. Local clocks assigned to one particular output can also affect other outputs, as well (related to having multiple Option Cards with multiple instances)
- 16) **(5/31/12 KW) LCD window keeps scrolling through data**, even though nobody is touching the keypad. We found the front panel ribbon cable is getting cut by the front panel metal, causing it to short out. Will be soon adding tape to the metal edges as a temp fix, until a permanent fix is put into place.
- 17) **Dropped packets on Gigabit Option Card (1204-06)**. Results in intermittent loss of all network communication. Reboot is a temporary fix. Refer to Morgan Stanley cases for more detail. A glitchy power save feature needed to be disabled with a bit in the FPGA. Fixed in 4.8.6 software update.
- 18) **PTP Option Card (1204-06)** Versions 4.8.5 and below: Cards respond to ping just fine from Windows PCs but not from Linux machines. Fixed in 4.8.6 update.

➤ GPS Survey is restarted in Standard mode after each reboot (noticed w/4.8.6 installed).

Refer to Mantis case 1734 for more info.

**Email from Dave Lorah to internal/engineering**

In today's 2:00 conference call with Hughes Network Systems I will tell them the problem turned out to be a software bug that occurs if switching to Mobile Mode after the GPS Survey is completed. Doing this corrupts the config files. This results in the unit sometimes restarting the survey after a power cycle.

There is a workaround where a Clean/Halt can be performed and this will solve the problem. But if placed in Mobile Mode after the survey is completed it will have the problem again.

Paul said this can be fixed for the next firmware release due in Sept/Oct.

**Email from Dave Lorah to Hughes (7/13/12)**

As we discussed yesterday, the problem with the Securesync restarting the GPS Survey after a power cycle is caused by a corruption of the configuration files. The files can become corrupted if the GPS Mode is changed from the default setting "Standard" mode to "Mobile" mode after the initial survey has been completed.

We are working on a correction for this and it should be included in the next scheduled firmware release. The release is scheduled for Sept/Oct 2012.

In the mean time we have a workaround to prevent the error from occurring and to correct any corrupted configuration files.

If the problem exists there is a way to clear the error from the config files in the Securesync. By performing a CLEAN/HALT function from the web browser the configuration files are cleared out and any erroneous files erased. This sets the unit to factory defaults.

Then you must avoid manually changing the GPS Mode to "Mobile" mode. You should not have to do this anyway. Just leave the unit at defaults and it will operate automatically.

To perform a CLEAN/HALT function:

Open the web browser for the Securesync unit

Navigate to the TOOLS/UPGRADE/BACKUP screen

Select the CONFIGURATION tab

Change the Clean/Halt field from Disabled to Enabled and select SUBMIT

This will clear out the configuration files and any erroneous settings. The unit will HALT operation and will need a power cycle to resume operation.

Issue with erratic System log entries in units with Rb oscillator installed (Applicable in at least v4.8.6)

➤ **(Refer to Mantis Case 1729)**

Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL\_Get - Label(oscillator\_ca\_dac0) - devindex(0) - index(4294967295) (WEB)  
Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL\_Get: SPEC\_KTSAL\_EN=true XO\_GetDac 0 (KTSAL)  
Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR

**(Network -> SNMP page, Notifications tab) SNMP “Version” field displays a “Null” when SNMPv3 is selected**

➤ (Reference Mantis case 1909) at least versions 4.8.7 and below.



Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
v1	Trap	trap	IPv4	10.2.100.29	162		None		None	
	Trap	snmptest	IPv4	10.2.100.29	162	0x8000168880	MD5	snmpstest	DES	snmpstest

## Models 9483 and 9489



- **Shortcut to Model 9400 series Manual:** <I:\New Released\Manuals\1209-xxxx-xxxx>
- **Shortcut to Model 9400 series sheet:** [I:\Marketing\ Product Data Sheets \(archive\)\Time & Frequency References](I:\Marketing\ Product Data Sheets (archive)\Time & Frequency References)
- **Shortcut to Model 9400 series firmware upgrades:** <I:\Customer Service\PSB, PSP software updates\948x and SecureSync>
- **Link to manual CD that we ship (1217-5003-0001):** <I:\New Released\Media> (includes manuals/quick start guides for 814x product, 9300 and 9400 series, TimeView display clocks, CTCSS and SecureSync)

### Last Time Buy (LTB) / End of Life (EOL) / Discontinuance of NetClock 9483/9489

- Letter of Discontinuance (Dated 20 Dec 2022) excerpted below and located in: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\948x discontinuance>

#### NetClock Discontinuance and Last Time Buy Notification

Dear valued customer and partner,

This notice is to inform you of the pending discontinuance of the **NetClock** time server. The NetClock is succeeded by the next generation enhanced **SecureSync 2400** which is available today .

This discontinuance notice applies to NetClock base units (9489 and 9483, bundles) and to a limited number of option cards and accessories. A detailed list is provided in appendix.

A Last Time Buy opportunity will be offered with following terms:

- LTB orders will be accepted from January 1<sup>st</sup>, 2023, to June 31<sup>st</sup>, 2023
  - Shipments of LTB orders can extend up to end 2023
- Due to limited part availability, orders will be honored only while supply is available.

NetClock technical support will be provided up to end of 2030. During the support period :

- Premium Support service contracts can be renewed
- Hardware repairs will be available based on component availability
- Software updates will be provided to support critical bugs and security vulnerabilities on an ad-hoc basis

Orolia encourages customers to migrate to the next generation SecureSync 2400 platform. SecureSync 2400 brings a range of improvements associated with networking, processing power, security and monitorability, while maintaining the flexibility and modularity that was part of NetClock. In addition, SecureSync 2400 offers more built-in outputs along with hot-swap power supplies for improved availability. In addition, for customer requiring compliance to NENA standard, a

new breakout cable is now offered, which provides compatibility with legacy NetClock NENA interfaces.

Orolia's Application Engineering team is available to guide you through the transition from NetClock to SecureSync 2400.

At Orolia, we provide our customers with the most resilient Position, Navigation, and Timing solutions and we continue to optimize our products by integrating the latest technology, leading the way to improved performances and capabilities.

Please feel free to contact your Orolia sales representative or myself for any additional information you would need.

Sincerely,

Emmanuel SICSIK-PARE  
*Strategic Product Manager,*

## Appendix

### Discontinued Part Numbers

Part Number	Comment
NetClock base units 9483 9489	
Options NetClock Opt 04 - Rubidium NetClock Opt 05 – OCXO NetClock Opt 13 – E1/T1 outputs NetClock Opt 14 – 12 VDC power NetClock Opt 15 – 24-48 VDC power NetClock Opt 32 – Gb PTP Master	
Packages GP230M-94 GP330M-94 GP933-NG911 GP933-MOT-NG911 GP934-NG911 GP951-NG911 GP951-MOT-NG911	

---

### Visio Stencils/shapes for the Models 9483 and 9489

- Refer to (on our website) <http://www.spectracomcorp.com/tabid/456/Default.aspx>
- Refer to: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\visio stencils>

**Email from Morgan (2 Feb 16)** Thank you for the questions about the Visio Stencils. We do have some (5) available, these have not been updated since 2013. Review the link below to see if we have what you need. We do have CAD drawings.

<http://spectracom.com/resources/product-documents>

Q from Keith to Tim K (1 Feb 16) We have a customer asking for Visio stencils for SecureSync. I have the following email and then the attached Front Panel from you, both back in 2013. Do you have anything more recent (such as rear panel), or is this still the same?

We do not have any visios built using our SecureSync, but I can share with you the attached portable network graphic file that I have used as a simple illustration. You can insert it into a visio document (or even any of our product photos from the web site) if you are looking for something generic. If you are looking for back panel detail to show connections, then you may need to create it yourself

A Reply from Tim K You are mostly correct, Keith. Nothing new since 2013. But everything I had that time is now available from within VSS files that can be downloaded from **Resources > Product Documents > Visio** <http://spectracom.com/resources/product-documents>

---

## Model 9489s

### (9489 versus SecureSync/9483)

#### All 9489s have:

- NTP, (2) RS-485 (Remote) ports, and (1) 1PPS out
- AC input power only (no DC input available)
- Only available with TCXO oscillator.

#### All 9489s don't have:

- Cooling fan/fan control functionality
- front panel keypad/LCD display
- 10 MHz output
- Capability to add Option Cards (such as multi-port Gigabit or IRIG input/output)
- Available DC input power
- Capability for OCXO or Rb oscillator upgrade
- Temperature sensor (U60) for the "oscillator temperature".

### 9489 with RS-485 input (replacement to the Model 9388s)

➤ Refer to **ECO-NPI-000879** in Arena ([https://app.bom.com/changes/detail-summary?change\\_id=2386349507&](https://app.bom.com/changes/detail-summary?change_id=2386349507&)) (Apr, 2017)

- This change will add an ASCII Input to the rear panel of the NetClock 9489 widening the 6-pin connector to 10-pins and adding pins 7-8-9 as the ASCII Input + - GND and Pin 10 as spare.

#### Findings about the chassis alignment of the pin label

1. The only finding with the FAI was that **the alignment of the G on pin 9 is too close and overhangs pin 10 on the connector. ECR-000187 written to request an improvement of labeling to more clearly make pin 9 G and pin 10 spare/unused.**

---

## Model 9483s

### (9483 versus SecureSync)

- 9483 is like a SecureSync, but ships with one NENA Option Card installed
- Unlike SecureSync, 9483 has a very limited list of available Option Cards that can be purchased with it.
- 9483 has two available Option Bays for adding additional cards.

**NENA Option Card (1204-1F) provides: (refer to SecureSync option card doc for more info on 1204-1F)**

**Note: Only one 1204-1F NENA card can be installed in each NetClock**

- A) One RS-485 and one RS-232 out
- B) two alarm relays (major and/or minor alarms - not an event relay)
- C) IRIG output
- D) 1PPS output

### Difference between SecureSync and 9400 series

Q Could you please give the real differences between the SecureSync line and the 94xx series other than the up-charge for saying the 94xx's are NENA compliant.

**A Partial reply from Jeremy Onyan (4 Feb 16)** ...Regarding your question about the differences between the two platforms, the difference depends on which 94xx you compare to the SecureSync. The 9489 is a no frills, low cost NTP time server. It comes with a TCXO oscillator and a static port configuration (you can't add / change outputs). The 9483 on the other hand, is the public safety specific platform. Under the hood it's the exact same everything as the SecureSync. However, it has a special NEMA module pre-installed which is needed for the public safety market. This NEMA module adds about \$1200 to the base cost and cannot be removed (otherwise it's then just a SecureSync with a different bezel). The 9483 also has only a handful of modules you can add to it, compared to the SecureSync which supports all of the timing modules.

So to sum things up, the 9489 is an entry level time server which doesn't have the features or specs you need (and they can't be added). And the 9483 is really just a SecureSync with a \$1200 module preinstalled that you don't need, with a different bezel, and limited ability to add / change modules.

---

## Power consumption/heat dissipation/Grounding and Power Supplies

- **Note:** Refer to SecureSync section of this document for more info: Input power (AC and DC)/ Current

### Power Draw/heat dissipation

- **TCXO: 40W** normal (**40W** start-up) **136.48566532** BTU/hr
- **OCXO: 40W** normal (**50W** start-up) **136.48566532** BTU/hr normal (**170.60708165** BTU/hr startup)
- **Rb: 50W** normal (**80W** start-up) **170.60708165** BTU/hr normal (**272.97133064** BTU/hr startup)

---

## PS06R-2Z1M-DT01 (Available AC to DC converter for redundant AC input)

- Refer to: Available AC to DC converter for redundant AC input (In the SecureSync input power section)

**Spectracom P/N:** PS06R-2Z1M-DT01



---

## MSF/WWVB/DCF77

### Email from Dave Sohn (7/24/12)

There are no plans for radio time signals like MSF, WWVB, and DCF77 in the SecureSync/NetClock 9400 products at this time. Our alternatives for GPS signal failure are to provide holdover during the failure period with our OCXO and Rubidium oscillator options, if they do not have supported alternative time signal sources available.

## Specific Options for 9483s only

- summary below, with details on some options further below

### Options summary for 9483 only

*Option 04:* Rubidium Oscillator

*Option 05:* OCXO Oscillator

Option 08: Commercial GPS receiver

Option 09: TCXO

*Option 12:* PTP I/O (via Option Card Model **1204-12**)

*Option 13:* T1/E1 outputs (via Option Card Model **1204-0A**)

*Option 14:* DC redundancy (**12vdc**)

*Option 15:* DC redundancy (**24-48vdc**) (add this option if its desired to connect PS06R-2Z1M-DT01)

*Option 16:* Multi-port Gigabit Option Card (adds three 10/100/1000 BaseT) (via Option Card Model **1204-06**)

Option 17: Programmable *TTL output card* (via Option Card Model **1204-??**)

---

### Options via rear panel Option cards

#### Option 12: PTP Input/output (Model 1204-12 PTP card)

- Refer to: Model 1204-12 PTP Option Card: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf>



---

#### Option 13: T1/E1 outputs (Model 1204-0A Option Card)

- Refer to: Model 1204-0A T1/E1 Option Card: <..\SecureSync Option Card information.pdf>

---

#### Option 14: Adds 12vdc input for redundancy

- Don't add Option 14 (12vdc input) if its desired to use our external power pack for "dual AC" input (like we periodically do with SecureSyncs)
  - The external power pack provides 24vdc output (not 12vdc)
  - Add instead Option 15 (24vdc input)

---

### Option 15: Adds 24vdc input for redundancy/ desire to use PS06R-2Z1M-DT01

- Add Option 15 (24vdc) if it's desired to apply our AC to DC converter for "dual AC" input.

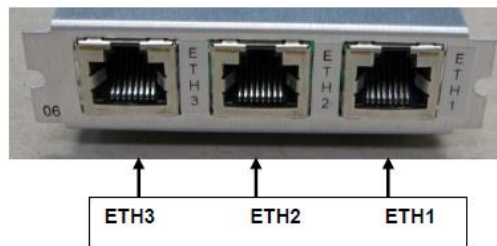


- The external power pack (our P/N **PS06R-2Z1M-DT01**) outputs 24vdc (not 12vdc)
- refer to (in this document): [\\*\\*\(PS06R-2Z1M-DT01\) Available AC to 24VDC converter for redundant AC input](#)

---

### Option 16: Multi-port Gigabit Option Card (adds three 10/100/1000 BaseT) (Model 1204-06)

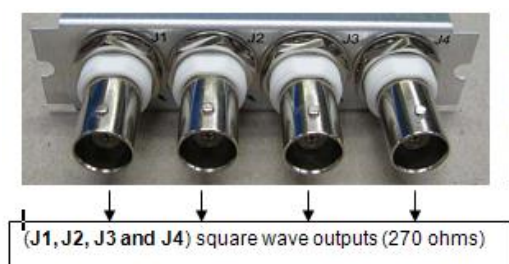
- Refer to: Model 1204-06 Gb Ethernet Option Card I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf



---

### Option 17: Programmable TTL output card (Model 1204-??)

- Refer to: (Model 1204- ) I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf



---

## Password reset when current spadmin password is not known Model 9489 only)

- Refer to Mantis 1967 (March 2013)

Because the 9489 has no keypad and because the front panel serial port is password protected, currently the only way to reset the password is to either replace the CF card to reset all of the configs or use remote desktop to login as spfactory (assuming no user has chosen to delete the spfactory account- if it has been deleted, a new CF card has to be sent and swapped in).

**Spfactory login: Tools -> Users page, Manage User Accounts tab**

Username	Group	Password	Retype Password	Update Account	Remove Account
spadmin	admin	*****	*****	<input checked="" type="checkbox"/>	<input type="checkbox"/>
spfactory	admin			<input type="checkbox"/>	<input type="checkbox"/>

Submit    Reset

Enter desired password    Click "Update Account"

---

## Network ports / configuration (IP address, gateway address,

**Important Note:** The Model 9489 is 10/100 base T only. There is no Option for it to have a Gigabit Option Card installed. So, it's limited to the Eth0 port on the chassis (which is 10/100 only). If 1000 base T is required, either a NetClock Model 9483 (with Option 16) or a SecureSync (with a Model 1204-06 Option Card) is required.

### Model 9489 Default Settings

**Note:** Eth0 only –this is a 10/100 port

- DHCP: disabled
- **Static IP address:** 10.10.201.1
- **Subnet mask:** 255.255.255.0

**To setup a static IP address, netmask, and gateway, in 9489 perform the following steps:**

1. Enter "**ip4set 0 address mask**", using your static IP4 address and net mask.
2. Enter "**gw4set 0 gw\_address**", using your gateway address **gw\_address**.

## Netmask settings

A Subnet mask converter for unique subnets <https://www.dan.me.uk/ipsubnets> . Enter one IP address and it will show you which other IP addresses are on the same subnet.

Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		




Table 2.3: Subnet mask settings

### Using ARP and ping to set the static IP address of a Model 9489 (no DHCP server available)

- Reference: <http://www.ipcas.com/support/developer/embedded-pc-linux-box/ip-address-setting-ipsetd.html>

**Note:** Process must finish within 5 minutes or the temporary address expires.

#### A) From a Windows or MS-DOS system:

- Start a DOS prompt (command shell)  
(For example: Start Execute cmd OK)
- Enter the following instructions:  
arp -s  
ping -l  
  
arp -s <IP-address> <Network Hardware Address (MAC address)>  
ping -l <length> <IP-address>
- For example:  
  
arp -s 192.168.1.45 00-09-8e-00-16-a3  
ping -l 408 192.168.1.45

#### B) With a UNIX or Linux system:

- Start a command shell
- Enter the following instructions as a user root:  
arp -s  
ping -l  
  
arp -s <IP address> <Network Hardware Address (MAC address)>  
ping -l <length> <IP address>
- For example:  
  
arp -s 192.168.1.45 00:09:8e:00:16:a3  
ping -l 408 192.168.1.45

## 948X Oscillators

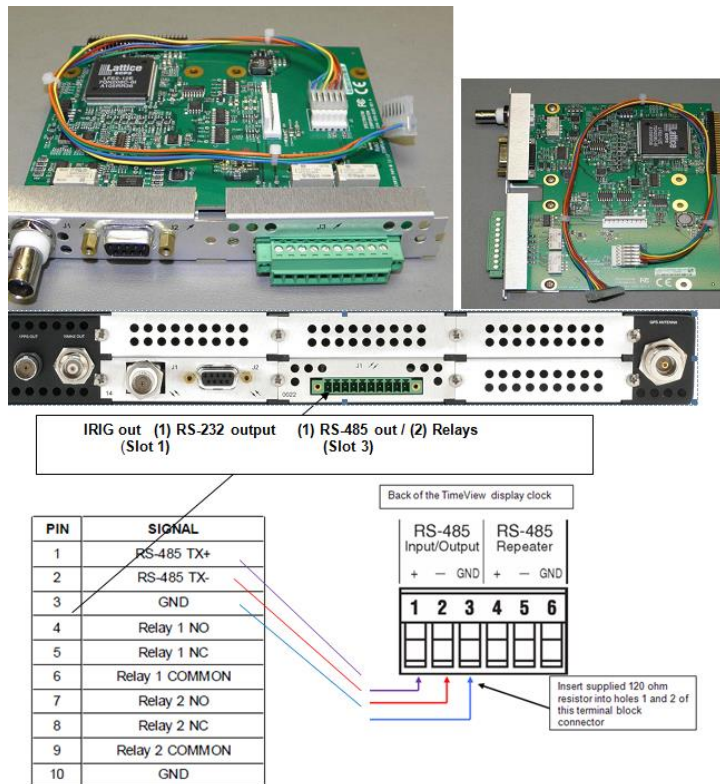
### Typical Holdover values

- TCXO (Standard)
- OCXO (Option 05)
- Rubidium (Option 04)

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium
<b>Holdover</b> (constant temp after 2 weeks of GPS lock)				
After 4 hours	12 $\mu$ s	1 $\mu$ s	0.5 $\mu$ s	0.2 $\mu$ s
After 24 hours	450 $\mu$ s	25 $\mu$ s	10 $\mu$ s	1 $\mu$ s

## NENA Option Card (RS-232 output, RS-485 output and IRIG output)

- Refer also to the SecureSync Option Card Document (its the 1204-1F Option Card)



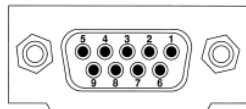
## 10 Pin Terminal block connector for 1204-1F (NENA) card



- **Our P/N:** J900R-0101-022J (in Arena) [https://app.bom.com/items/detail-spec?item\\_id=1202843926&version\\_id=10303495198](https://app.bom.com/items/detail-spec?item_id=1202843926&version_id=10303495198)
- **Manufacturer and MFG P/N:** Phoenix Contact, P/N 1827787
- Refer to: <https://www.phoenixcontact.com/online/portal/us/?uri=pxc-oc-itemdetail:pid=1827787&library=usen&pcck=P-11-02-11&tab=1&selectedCategory=ALL>

## RS-485 pin-out when replacing NetClock/2 with a Model 9483

**Email from Keith (18 May 16)** Per our conversation and your request, below is information on moving the RS-485 Remote output wiring from a NetClock/2 over to the new Model 9483. As you can see below, the RS-485 out of a NetClock/2 is on a DB9 connector and a terminal block on the Model 9483. Migrating the NetClock/2's Remote output to the Model 9483's Remote port consists of removing the DB9 connector and inserting the wires that were on pins 3, 8 and 9 of this connector into the left three pins of the terminal block on the back of the Model 9383. Note the wires should be stripped of insulation before inserting the wires and tightening the screws on the top of the terminal block connector.



Signal	NetClock/2 RS-485 Remote Output port (DB9F connector)	Corresponding Color of wire inside Modular jack (telephone jack) if present	Pin on Model 9483s rear panel terminal block connector (starting from the left side)
+Data	Pin 3	Green wire	Pin 1
-Data	Pin 8	Red wire	Pin 2
Ground	Pin 9	Yellow wire	Pin 3

## ASCII RS-485 ("ASCII output 1") Output configuration

### A) Newer browser

- Refer to online 9483 user guide at: [http://manuals.spectracom.com/NC/Content/NC\\_and\\_SS/Com/Topics/OPTCARDS/OC\\_QRG/ConfigSets\\_IO.htm](http://manuals.spectracom.com/NC/Content/NC_and_SS/Com/Topics/OPTCARDS/OC_QRG/ConfigSets_IO.htm)

#### Note

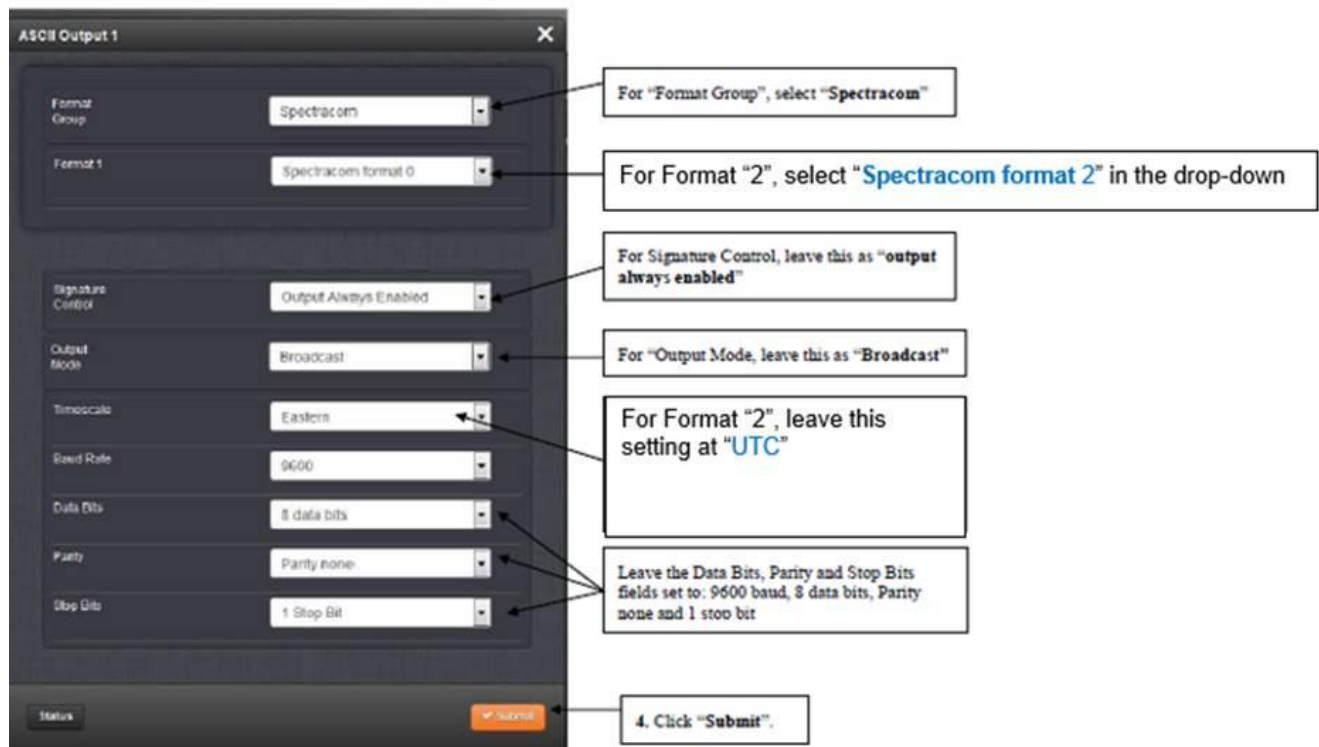
- **Interfaces** -> **ASCII Output 1** = RS-485 port
- **Interfaces** -> **ASCII Output 0** = RS-232 port

To output ASCII Data Format 2 from the left two pins (pin 3 is ground) of the green connector on the back of the Model 9483:

Navigate to the **Management -> Interfaces -> ASCII Output 1** page of the NetClock's web browser (you can select "**ASCII Output 1**" under either "**ASCII output**" or "**NENA**" in the "**Interfaces**" drop-down). Then press "**Edit**" in the pop-up window that opens. This will open the Configuration menu (as shown further below). Configure this pop-up window, as indicated, and then press Submit.

**Note:** For more info on configuring the Remote RS-485 port (referred to as "**ASCII output 1**") refer to the online Model 9483 user guide at:

[http://manuals.spectracom.com/NC/Content/NC\\_and\\_SS/Com/Topics/OPTCARDS/OC\\_QRG/ConfigSets\\_IO.htm](http://manuals.spectracom.com/NC/Content/NC_and_SS/Com/Topics/OPTCARDS/OC_QRG/ConfigSets_IO.htm)



After pressing Submit, the green, rear panel terminal block connector on the will start sending out ASCII Format 2 data, once-per-second.

Note the green terminal connector (starting from the left-most pin, as looking at it from the rear panel ) is pinned as follows: **+ - Ground**. Make sure that the + goes to the + on the Model 8180, - goes to -, and ground goes to ground. Incorrect pinning wont damage any equipment, but will prevent the Model 8180 from syncing to the Model 9483.

## B) Classic interface browser

- **Setup -> Outputs -> Slot 3** ("ASCII RS-485 & Relays") page of the browser

ASCR RS-485 Relays	
Signature Control	Output Always Enabled
First Format	Spectracom Format 2
Second Format	None
Third Format	None
Mode	Broadcast
Time Scale	UTC
Local Clock	UTC
Baud Rate	9600
Data Bits	8 Data bits
Parity	Parity none
Stop Bits	1 Stop bit

## ASCII RS-232 Output configuration

- Setup -> Outputs -> Slot 1 ("IRIG & ASCII RS-232") page of the browser

OUTPUTS SETUP - IRIG AND ASCII RS-232 TIMECODE (SLOT1)	
ASCR RS-232	
Signature Control	Output Always Enabled
First Format	None
Second Format	None
Third Format	None
Mode	Broadcast
Time Scale	UTC
Local Clock	UTC
Baud Rate	9600
Data Bits	8 Data bits
Parity	Parity none
Stop Bits	1 Stop bit

## IRIG Output configuration

- Setup -> Outputs -> Slot 1 ("IRIG & ASCII RS-232") page of the browser

OUTPUTS SETUP - IRIG AND ASCII RS-232 TIMECODE (SLOT1)	
ASCR RS-232	
Signature Control	Output Always Enabled
Format	IRIG-B
Blockcode	17 995.88
Control Sequence	11 995.88 CP
Control Field	RDC 200-54
Time Scale	UTC
Local Clock	UTC
Baud Rate	9600
Data Bits	8
Parity	Parity none
Stop Bits	1

## Desire to add additional NENA cards for more relays and outputs

Customer can add a second NENA Option Card, which provides four Minor/Major alarm relays (but software only allows control of the first three relays – the fourth won't be useable)

## Software versions/updates/issues

**First version of software for the Model 9483:** The Model 9483 was first cut-in with the version 4.6.0 release.

## System Logs

All NetClock Logs are stored in the **home/spectracom/log** directory.

-Starting in version 4.7.0, All Logs can be placed into a single log file and then exported out using FTP/SCP: The log bundling is controlled in the **"Tools"/ "Upgrade/Backup"** page of the NetClock's web browser. Click on the "Configuration" tab. Then, to bundle the logs, change "Save Log Files" to "Enabled" and then hit Submit. This generates a single file bundle of the logs. This file ("netclock.log") is placed in the **"home/spectracom/xfer/log"** directory. Once it has been created, you can FTP/SCP it off the box (just make sure "FTP Service" is enabled in the Network/General page of the browser, "Services" tab).

If you need a free FTP client, we often use CoreFTP: <http://www.coreftp.com/>

## A) Software issue causing System Log to become full of GPS Monitor daemon entries



- Refer to Mantis case 0002398 <http://cvsmantis.int.oroia.com/mantis/view.php?id=2398>)
- Per NC Number 7252: With units that don't have a GPS receiver installed - System Log shows GPS Monitor daemon starting and terminating from time of power up. This effects releases 5.0.0 thru 5.0.2.

---

### **SNMP (MIBs/Traps/OID Numbers/Email Alerts)**

- Refer to SecureSync SNMP section in this document for more info: SNMP/MIBS/OID NUMBERS/Email Alerts
- The MIB files and SNMP traps for the 948x products are the same as for the SecureSync.

**Note:** NetClock 948X customers (Upgrading from NetClock to SecureSync) will need to load and use the SecureSync MIBs. Customers with both the 948x and installed bases of 938x and 928x will need to use BOTH the NetClock 938x/928x MIBS and the SecureSync MIBs.

---

### **Local System Clocks (Local Clock)**

- Refer to **Local Clocks** in SecureSync directory: [Local System Clocks \(Local Clock\)](#)