

VersaSync/VersaPNT (1228s) assistance

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

Table of Contents

OGSI SUPPORTED PRODUCTS	6
SAFETY: UL / FCC/ EMC-ESD / EMI / CB TESTING / ROHS-CE / COMPLIANCE / DECLARATION OF CONFORMITY (DoC)/IEC-60950-1/IEC-62368 6	
CE DECLARATION OF CONFORMITY (DoC) FOR VERSASync/VERSAPNT (NEEDS TO BE UPDATED FOR “VERSA”)	7
LEAKAGE CURRENT (CURRENT LEAKAGE) (INFO NEEDS TO BE UPDATED FOR “VERSA”)	8
FLAMMABILITY TESTING/CERTIFICATION (INFO NEEDS TO BE UPDATED FOR “VERSA”)	8
EMI-EMISSIONS/EMC/ESD TESTING (INFO NEEDS TO BE UPDATED FOR “VERSA”)	9
UL TESTING/ UL CERTIFICATES (INFO NEEDS TO BE UPDATED FOR “VERSA”)	9
***TOUCH CURRENT (INFO NEEDS TO BE UPDATED FOR “VERSA”)	9
ROHS COMPLIANCY STATEMENT FOR VERSASync/VERSAPNT.....	10
MIL-STD-461 (ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS).....	10
DISA/STIG (SECURITY TECHNICAL IMPLEMENTATION GUIDE) FOR ALL PRODUCTS.....	11
INFORMATION ASSURANCE (IA) / COMMON CRITERIA (CC) / EAL LEVELS	13
CIP/CYBER SECURITY/POTENTIAL VULNERABILITIES/ANTI-VIRUS SOFTWARE	14
FIPS COMPLIANCY (FIPS 140-2) FOR ALL SPECTRACOM NTP SERVERS	16
**GENERAL RECOMMENDATIONS FOR VULNERABILITY TESTING.....	17
PCI-DSS / PCI COMPLIANCE (PAYMENT CARD INDUSTRY) SECURITY ASSESSMENTS/AUDITS.....	19
ISO 8601 (ISO-8601) COMPLIANCY	22
IEC 61850 (ELECTRICAL SUBSTATION AUTOMATION SPECIFICATIONS)	22
VOLUNTARY PRODUCT ACCESSIBILITY TEMPLATE (VPAT)”.SECTION 508 FORM / FORM 508 OF THE REHABILITATION ACT (FOR PEOPLE WITH DISABILITIES: BLIND, HEARING IMPAIRED. ETC)	22
JAPANESE SAFETY COMPLIANCE	23
SCADA SYSTEMS	24
Y2K38 (YEAR 2038 ROLLOVER) (“UNIX MILLENNIUM BUG”).....	24
VERSASync/VERSAPNT (“1228” COMPACT / RUGGEDIZED “SECURESync”)	25
*SHORTCUTS/LINKS (DATASHEET/SCHEMATICS/QUICKSTART GUIDES/PROCESS DETAILS)	27
FACTORY WARRANTY PERIODS	27
SPECTRACOM PRODUCT ROADMAPS	27
CE DECLARATION OF CONFORMITY (DoC) FOR VERSASyncs.....	28
CAD/3D DRAWINGS FOR VERSASync	28
PRODUCT SPECIFICATIONS/MOUNTING THE VERSASync.....	28
***ENVIRONMENTAL SPECS.....	28
**MOUNTING/MECHANICAL SPECS (SIZE, MOUNTING AND DIMENSION/ TOLERANCES INSTALLATION DRAWING)	28
GROUNDING.....	29
**{SHOCK/VIBE (MIL-STD-810F).....	29
VERSASync EVALUATION KITS (VEK).....	30
VERSASync/VERSAPNT OPTIONS	34
A) VP-OPT-BSH: VERSA FAMILY INTERFERENCE DETECTION SUITE OPTION	34

VERSASync OPTION CARD	47
CHASSIS RELATED / MOUNTING.....	47
***MOUNTING PLATE/HOLES.....	47
(1226-1000-9701) METAL PLATE ON BOTTOM OF CHASSIS.....	47
(1226-1000-9703) TOP COVER.....	47
RUGGEDIZATION TESTING (MIL-STD-810G/MIL-STD-461F).....	48
IP64 RATING/IP65 PLUGS FOR VERSASync SAASM AND SMA HOLES	48
VERSASync/VERSAPNT MODEL NUMBERING SCHEME.....	49
INERTIAL NAVIGATION/IMU (INERTIAL MEASUREMENT UNIT) FOR VERSAPNTS.....	51
LEVER ARM	52
KALMAN FILTER.....	52
REAL TIME CLOCK (RTC) AND RTC RECHARGEABLE LITHIUM BATTERY (BT1)	53
OPTIONAL STANDBY MODE AND POWER-UP (VSTANDBY).....	57
POWER/STATUS LEDs	58
TEMPERATURE/TEMPERATURE MONITORING/HIGH TEMPERATURE ALARMS DETECTED	62
*INTERFACES/CONNECTORS/CABLES (CABLING)	64
INFO FOR ALL CONNECTORS/INTERFACES.....	64
VERSASync BREAKOUT CABLES.....	66
AVAILABLE PROTECTIVE DUST CAPS KIT (AKA ODU AMC SOAK CAPS).....	66
AVAILABLE "VERSASync MATING CONNECTORS KITS"	67
SUMMARY OF THE VARIOUS TIMING INPUT/OUTPUT SIGNALS ("TIMING INTERFACES")	68
FRONT PANEL CONNECTIONS.....	70
*INPUT POWER CONNECTOR/STANDBY POWER (INPUT POWER CONNECTOR AND MIL-STD STANDARDS FOR POWER)	70
DOD MILITARY STANDARDS FOR INPUT POWER (SUCH AS MIL-STD-1275 AND MIL-STD-704)	73
**ETHERNET INTERFACE (ETHERNET) CONNECTOR	76
**ETHERNET BREAKOUT CABLE (CA08R-CRET-0002) FOR ETH0 AND ETH1	78
FOUR WIRE 100 MB ETHERNET CONNECTION ONLY (NOT FOR USE WITH 1GB CONNECTIONS)	79
**MULTI "I/O" CONNECTOR (INPUTS/OUTPUTS, SUCH AS USB/SERIAL FOR CLI INTERFACE, 1PPS, ASCII, IRIG, ETC)	81
I/O SIGNAL MAPPING TABLE	84
INTERACTIVE I/O CONFIGURATOR	85
MULTI I/O CABLE (USB CONNECTOR FOR TERMINAL CONNECTION) AND I/O BREAKOUT CABLE	87
INPUTS	89
****IRIG INPUTS/OUTPUTS	89
***1PPS INPUT	100
***HAVEQUICK/STANAG INPUT.....	101
***ASCII INPUT	102
GPI PINS (GPIO).....	103
***PTP INPUT (PTP SLAVE)	103
OUTPUTS	104
(ONE OR FOUR 10 MHZ OUTPUTS).....	104
*1PPS OUTPUT / xPPS OUTPUT	106
***ASCII OUTPUT	108
***HAVEQUICK/STANAG OUTPUT.....	109
GPO PINS (GPIO).....	110

PTP MASTER / PTP OUTPUT (ETH1 ONLY).....	110
SUPPORT OF PTP OVER VLAN	110
ITU-T STANDARDS FOR PTP (SUCH AS SYNCE).....	110
PTP INPUT (PTP SLAVE MODE) CONFIGURATION/OPERATION	111
PTP OUTPUT CONFIGURATION/OPERATION	112
PTP OUTPUT WEB BROWSER PAGE/TABS (VERSIONS 1.4.0 AND BELOW)	113
PTP OUTPUT CONFIGURATION.....	117
SOFTWARE FIXES/KNOWN ISSUES WITH PTP OUTPUT (PTP OPERATIONS) PRIOR TO VERSION 1.5.0.....	121
** CHRONY NTP OUTPUT (“NTP SERVER”).....	123
***ASCII SERIAL OUTPUTS	127
NMEA OUTPUTS (GGA/RMC/ZDA)	127
NMEA FIELDS: MAGNETIC VARIATION/SPEED OVER GROUND/COURSE OVER GROUND.....	127
NEW FEATURE: NMEA-OVER-UDP FUNCTIONALITY.....	127
STANAG/HAVEQUICK OUTPUT	127
***USB/SERIAL INTERFACE FOR CLI CONNECTION / USB DRIVER	129
CLI INTERFACE (COMMAND LINE INTERFACE).....	130
“vi” TEXT FILE VIEWER/EDITOR.....	130
CTL LINUX COMMANDS (JOURNALCTL, SYSTEMCTL)	133
**OPTIONS CONNECTOR (OPTIONAL I/O CONNECTOR).....	137
EMMC FLASH MEMORY – NO COMPACT FLASH (CF) CARD INSTALLED IN VERSASYNC/VERSAPNT.....	137
SANITIZATION/CERTIFICATE OF VOLATILITY (COV) / LETTER OF VOLATILITY (LOV).....	138
NUMBER OF AVAILABLE DCLS TTL OUTPUTS.....	140
INPUT REFERENCES.....	141
**CHRONY NTP INPUT REFERENCE (NTP PEERING/NTP SERVER MODES FOR “STRATUM 2” SYNC).....	141
**PTP INPUT REFERENCE (PTP SLAVE MODE).....	141
**ASCII INPUT REFERENCE (RS-485 AND/OR RS-232 INPUT/ASCII TIME CODE).....	142
**HAVEQUICK INPUT REFERENCE (HQ INPUT 0”) INTO VERSASYNC	143
**1PPS INPUT REFERENCE (“EPP0”) INTO VERSASYNC	144
*(J1) GNSS/GPS (UBLOX RECEIVER) AND SAASM GPS.....	145
GPS/GNSS RECEIVER IS “RECEIVE-ONLY” (IT DOESN’T TRANSMIT)	145
M-CODE (M CODE) RECEIVER/CAPABILITIES	147
DEPT OF DEFENSE FORM DD-1494 (DD1494 FOR SAASM).....	147
GPSD (A GPS SERVICE DAEMON) (APPLICABLE TO VERSIONS 1.3.1 AND ABOVE ONLY).....	151
NAVIGATIONAL/MOTION (VELOCITY) VALUES OBTAINED USING GPSD.....	153
QUERYING/OBTAINING THE CURRENT UTC OFFSET FROM A VERSASYNC.....	153
DAGR/ICD-GPS-153C BI-DIRECTIONAL INTERFACE	153
10 MHZ OSCILLATOR (OCXO) / CSAC MAC (MICRO ATOMIC CLOCK), OR WENTZEL OSCILLATOR.....	155
ACCURACY SPECS/HOLDOVER / HOLDOVER SPECS	155
DISCSTATS FILES	157
SOFTWARE/SOFTWARE UPDATES/SOFTWARE DOWNGRADE	159
***CAN BUS INTERFACE (FOR VEHICLE INFORMATION INPUT).....	161
***VICTORY INTERFACES (VEHICULAR INTEGRATION FOR C4ISR/EW INTEROPERABILITY) FOR VERSAPNTS	161
NETWORK RELATED (ETH0 AND ETH1).....	163
**GENERAL NETWORK SETTINGS	163

NETWORK PORTS (INTERFACES ETH0 AND ETH1)	163
**MAIN "DEFAULT IP4 PORT" (MAIN DEFAULT IPv4 INTERFACE - MAIN DEFAULT IPv4 GATEWAY)	165
ETHERNET MONITOR PAGE AND GRAPHS	166
NETWORK SERVICES (TELNET/SSH, FTP/SCP, HTTP/HTTPS, TCPDUMP)	167
**SSH/SCP AND FTP/SFTP, ETC)	167
APACHE WEB BROWSER RELATED	168
***USER ACCOUNTS/ACCOUNT NAMES/PASSWORDS	168
***"WEB UI TIMEOUT /WEB BROWSER IDLE LOGIN TIMEOUT (LOGIN TIME-OUT AFTER NO ACTIVITY)	168
WEB BROWSER CACHE ISSUE (NEED TO PERIODICALLY CLEAN BROWSER'S COOKIES/CACHE)	169
***REST API INTERFACE/POSTMAN (ALTERNATE TO USING THE STANDARD WEB BROWSER OR CLI)	170
MANAGEMENT MENU PAGES	180
**MANAGEMENT -> TIME MANAGEMENT PAGE / LOCAL CLOCKS	180
**SYSTEM TIME/YEAR AND SYSTEM TIMESCALE	180
SYSTEM YEAR / "SET YEAR ONLY" CHECKBOX/FIELD	180
**LOCAL SYSTEM CLOCKS (LOCAL CLOCK)	181
**SYSTEM TIME MESSAGE DAEMON (STMD)	184
INTERFACES MENU	185
LOGS/SYSLOG	186
LOG REQUIREMENTS FOR PCI-DSS/ PCI COMPLIANCE	196
MISSING EXPECTED LOG ENTRIES/"SEARCH" FIELD FOR THE LOGS (TOP RIGHT OF THE INDIVIDUAL LOG PAGES)	197
REPORTING OF MODEL AND VERSION IN THE LOGS/LOG CAPTURE	198
**ABILITY TO VIEW THE LOGS (LOG ENTRIES) WITH CLI INTERFACE	198
**ABILITY TO DELETE THE LOGS	198
LOG CONFIGURATION/MAPPING (FACILITY AND SEVERITY CODES)	201
***DELETING/CLEARING LOG FILES	204
AVAILABLE LOG FILES IN 1232 VELASYNC	206
SYSTEM MESSAGES	207
NOTIFICATIONS / EMAIL ALERTS /SNMP	208
*NOTIFICATIONS (SNMP TRAPS AND EMAIL ALERTS)/ALARMS	208
OPT-IDM: AVAILABLE BROADSHIELD NOTIFICATIONS (v5.7.1 AND ABOVE ONLY, AND ONLY WITH OPT-IDM ENABLED)	210
**NULLMAILER/EMAIL ALERTS	213
**SNMP (SNMPv1/SNMPv2C/SNMPv3)	218
**REMOTE MONITORING / SNMP CONFIGURATION	219
***SYSOBJECTID, SYSCONTACT AND SYSLOCATION FIELDS	230
SYSNAME FIELD (UNIT'S HOSTNAME IN SNMP)	230
CPU USAGE (CPU USED) / PROCESSOR USAGE/CPU USAGE 100%	232
**USING LINUX TO PERFORM SNMPWALKS SNMPGETS SNMPTRAPS	235
USING SNMPGET COMMAND VERSUS USING EITHERSNMWALK/SNMPGETNEXT COMMANDS (FOR RETRIEVING VALUES FROM AN SNMP TABLES)	235
SNMPv3 ENCRYPTION INFO/DETAILS	243
SNMPv3 ENGINE ID FIELD	246
**TESTING/VERIFYING SNMP/EMAIL ALERTS ARE ENABLED AND WORKING INSIDE THE SECURESYNC	251
**TROUBLESHOOTING / KNOWN ISSUES WITH SNMP	253
EXAMPLES OF AVAILABLE SNMP GETS/SETS	262
PTP MIB FILE (FOR 1204-12 10/100 CARD) AND GB PTP MIB FILE (FOR 1204-32 CARD)	262

NOTIFICATIONS/TRAPS FOR SAASM RECEIVER ONLY..... 269
TESTING SNMP TRAPS AND EMAIL ALERTS..... 270

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.

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

Chatter Message from Jon Sinden 14 Dec 2018) Congratulations to the Rochester and Les Ulis engineering teams for passing VersaSync EMI/EMC compliance testing! The VersaSync now has certified test results for MIL-STD-461G tests CE101, CE102, CS114, CS115, CS116, RE101, RE102, RS101, and RS102. This allows us to capture key near-term orders and positions us well in the military vehicular equipment market. Military EMI/EMC compliance is very difficult to design for and our developers should be applauded for their hard work and perseverance!

The test report is available in Arena PLM under [DEC-CONF-VERSASYNC](#)

- 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](#)
- 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\EMC -CE Declaration of Conformity](#)

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

CE Declaration of Conformity (DoC) for VersaSync/VersaPNT (needs to be updated for “Versa”)

- DoC

A) VersaSync/VersaPNT CE approval/Declaration of Conformity (info needs to be updated for “Versa”)

- The VersaSync/VersaPNT is CE compliant, so a CE 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.

Leakage current (current leakage) (info needs to be updated for “Versa”)

- 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/>

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.

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 (info needs to be updated for “Versa”)

- 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 retardant 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, phosphonates as well as red phosphorus that can be used as flame retardant in PCBs.

EMI-Emissions/EMC/ESD testing (info needs to be updated for “Versa”)

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 (info needs to be updated for “Versa”)

- 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 (info needs to be updated for “Versa”)

- 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.

RoHS compliancy statement for VersaSync/VersaPNT

- 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

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
- Refer to the online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/VSS/INTRO/VSS_Compliance.htm

Details

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

FAQs

Note: the following Questions/answers were exported from the SecureSync assistance document (may be different for Versa).

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.

DISA/STIG (Security Technical Implementation Guide) for all products

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%5Fflayouts%2Flanding%2Easpx%3FSource%3Dhttps%253A%252F%252Fforoliagroupemicrosoftonlinecom%252D1%252Esharepoint%252Eemea%252Emicrosoftonline%252Ecom%252F%255Fforms%252Fdefault%252Easpx&lc=1033&id=500046&cbcxt=mai&wliidp=1&quest=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

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.

CIP/Cyber Security/Potential Vulnerabilities/Anti-virus software

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

- Refer to <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
- list of various Standards for the Power industry/Power grid

A) 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-Security-Compliance-Report.pdf” at the following link: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Security- Vulnerabilities](#)

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.

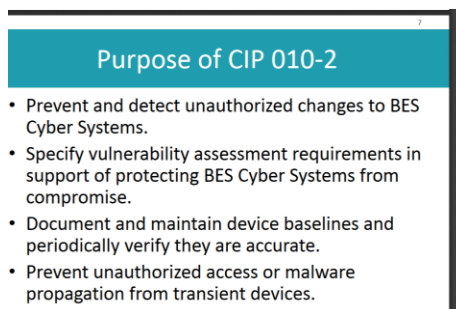
In general, we take in security vulnerability reports from our own scanning, from customers, and from vulnerability databases. Generally, these are handled within our quarterly releases. We try to provide workarounds in the mean-time, however, if necessary we can do an out of band release to resolve.

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

B) CIP-010 (CIP-10) 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 is 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 **saveconfig**<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).

FIPS compliancy (FIPS 140-2) for all Spectracom NTP servers

➤ Refer also to the “FIPS compliancy” section of [..\CustomerServiceAssistance.pdf](#)

Q. I was asked by our customer at the US Patent Office if the 9289 was FIPS compliant. I found no indication we have ever advertised the 9289 as being FIPS. Do any of you know if we do or do not say we are FIPS Compliant as far as the NTP MD5 Authentication goes?

A. Email response from Bill Glase (2/28/11) We are compatible with FIPS 140-2 compliant systems, but the certification does not apply to our device because [SecureSync] does not store or process user data (the FIPS 140-2 is a specific third-party certification that qualifies a cryptographic module to handle data).

By the way, MD5 (as used in the NTPv4 standard) is NOT a FIPS certified algorithm - so if the network time data were required to be FIPS certified for some particular system, it would require a custom protocol on both the client and server side.

Information below from: http://en.wikipedia.org/wiki/FIPS_140-2

Purpose

The [National Institute of Standards and Technology](#) (NIST) issued the [FIPS 140](#) Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Federal agencies and departments can validate that the module in use is covered by an existing [FIPS 140-1](#) or FIPS 140-2 certificate that specifies the exact module name, hardware, software, firmware, and/or applet version numbers. The cryptographic modules are produced by the [private sector](#) or [open source](#) communities for use by the U.S. government and other regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate [sensitive but unclassified](#) (SBU) information. A commercial cryptographic module is also commonly referred to as a [Hardware Security Module](#).

FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Level 2

Security Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and [critical security parameters](#) (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

Level 4

Security Level 4 provides the highest level of security.

At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs.

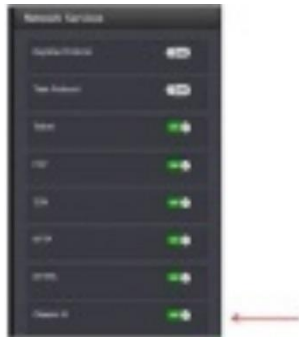
Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the

normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroize CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

****General recommendations for vulnerability testing**

- 1) 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?

PCI-DSS / PCI compliance (Payment Card Industry) Security Assessments/audits

Available Info:

A) websites such as:

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

B) links on our website on PCI- DSS.

<https://spectracom.com/customsearch?nocache=1528288286&searchText=PCI+DSS&offset=0>

https://spectracom.com/sites/default/files/document-files/PCI%20DSS%20Compliance_revB.pdf

C) emails and docs in:

- [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](#)

D) 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>

E) Salesforce cases, such as

164874

A vulnerability scanner can detect/report PCI DSS Compliance

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):

33929 - 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 Perimeter Service Plugin, and if you disagree with the results, you may submit this 'Submit for PCI Validation' and dispute the findings through our web interface.

See Also
<http://www.pcisecuritystandards.org>
http://en.wikipedia.org/wiki/PCI_DSS

Risk Factor
High

Plugin Information:
Publication date: 2008/08/07, Modification date: 2012/04/27

Ports
tcp@

3 medium risk flaws were found. See:
<http://www.nessus.org/plugins/index.php?view=logs&id=58751>
<http://www.nessus.org/plugins/index.php?view=logs&id=57582>
<http://www.nessus.org/plugins/index.php?view=logs&id=51192>

25220 - 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 compliance:

- 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)
 - 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

- 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 61850 (electrical substation automation specifications)

- Refer to "IEC 61850" in the custserviceassistance document.

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

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.

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

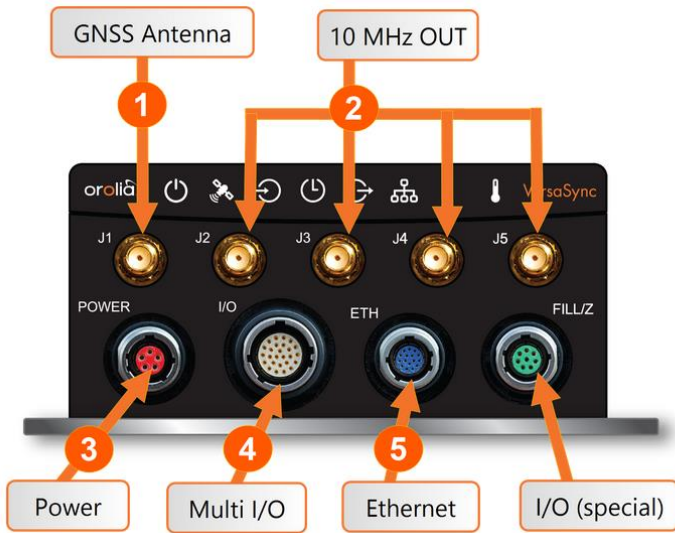
- **SCADA Stands for:** Supervisory Control and Data Acquisition (SCADA)
- **HMI:** Human Machine Interfaces
- **Points / Data Points** To the application developer the network represents itself as a set of elementary data elements, called data points (or simply points). These data points are the logical 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

VersaSync/VersaPNT (“1228” compact / ruggedized “SecureSync”)

A) VersaSyncs



B) VersaPNTs (shown with older labels)



*Shortcuts/Links (Datasheet/Schematics/quickstart guides/process details)

Datasheets

- **VersaSync datasheet** on our website: file:///C:/Users/Keith.Wing/Downloads/VersaSync-Rugged-Time-and-Frequency-Reference_11-17-2020_0-1.pdf
- **VersaPNT** on our website: <https://www.rolia.com/products/product-index/documents/versapnt>

Schematics

Main/Front panel (1228-1001-0200) in Arena at: <https://app.bom.com/items/detail...>

User Manual/quickstart guides

- **Online user manual** <http://manuals.spectracom.com/VSS/Content/VSS/INTRO/GettingStarted.htm>
- **User Manual** (1228-5000-0050) in Arena at: <https://app.bom.com/items/detail...>
- **Manual CD assembly** (1228-5003-6001) in Arena at: <https://app.bom.com/items/detail...>
- **Quickstart guides** (2)
 - Longer of the two (1228-5000-0051) in Arena: https://app.bom.com/items/detail-spec?item_id...
 - Four page (1228-5000-0056) in Arena: <https://app.bom.com/items/detail...>

Process Details (in Arena)

*General Info

- Jan 2017, ECO 1114 releases to Mfg four configurations (1228-0110, 1228-0410, 1228-1110 and 1228-1410)
- Engineering VersaSync available at: <https://10.10.224.49>

Factory Warranty periods

- 2-year warranty on VersaSyncs/VersaPNTs

Spectracom Product roadmaps

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

CE Declaration of Conformity (DoC) for VersaSyncs

VersaSync CE approval/Declaration of Conformity

- The VersaSync is CE compliant, so a Declaration of Conformity is available upon request.
- The “Declaration of Conformity” document (DEC-CONF-VersaSync”) is stored in Arena at: https://app.bom.com/items/detail-spec?item_id=1232126499&version_id=10760216368
- (Regarding Securesync- not positive on VersaSync) 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.

CAD/3D drawings for VersaSync

- CAD (3D .stp files) on our on website: <https://spectracom.com/support/versasync-support> (scroll down towards bottom of the page)
- Refer to: S:\Projects\Sketch_matchbox\Mechanical\3D Files for Customers and <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\VersaSync\drawings>

Email from Scott Holmes (24 Janx 17) Mike Messina asked for these yesterday. I placed the latest version here:

T:\Engineering\Projects\Sketch_matchbox\Mechanical\3D Files for Customers. My T drive is the ics drive.

I included a jpeg in the folder so you can see what the 3D files look like. They only need one of the two types of files (either a stp or igs). If they don't specify, send them a stp file.

CAD drawing for the mounting plate: refer to “Mounting plate” below

Product Specifications/mounting the VersaSync

***Environmental Specs

- Environmental test data reports (in Arena as “DOC-000127”): https://app.bom.com/changes/detail-summary?change_id=2390624476&
- Refer to online VersaSync User guide: http://manuals.spectracom.com/VSS/Content/VSS/INTRO/VSS_Specs.htm

**Mounting/Mechanical Specs (Size, Mounting and dimension/ tolerances installation drawing)

- Refer to online VersaSync user guide at:
 - http://manuals.spectracom.com/VSS/Content/VSS/INTRO/Specs_MechEnv.htm
 - <http://manuals.spectracom.com/VSS/Content/VSS/SETUP/Mounting.htm>
 - Expand the small drawing under “**Dimensions**” to expand the drawing

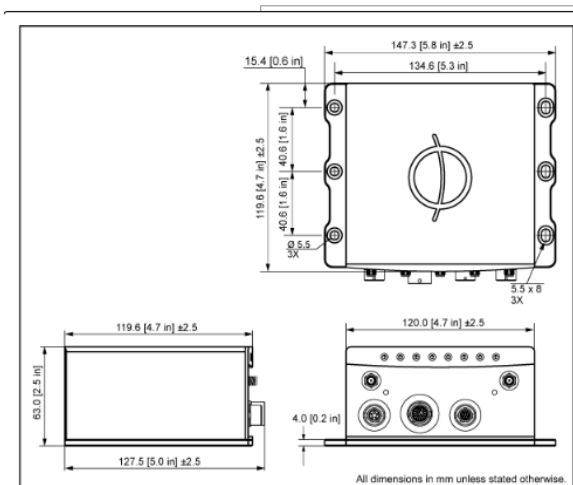
Physical Specifications

- **Dimensions (W x D x H): 147.3 x 127.5 x 63.0 mm (5.8 x 5 x 2.5 in)**



Mechanical dimensions

- **Mounting:** Bolted to a metal plate, using 6 through holes
- **Weight:** 0.91 kg (2.0 lbs)



Grounding

Refer to “**Grounding**” in online VersaSync user guide at <http://manuals.spectracom.com/VSS/Content/VSS/SETUP/Mounting.htm>

****(Shock/vibe (MIL-STD-810F)**

- Refer to online VersaSync User guide: http://manuals.spectracom.com/VSS/Content/VSS/INTRO/VSS_Specs.htm
- **Vibration:**
 - 7.7 g rms, 20 to 1000 Hz (in accordance with MIL-STD 810G, Method 214.6 Category 24: Minimum Integrity and Helicopter Minimum Integrity, see graphs 514.7E-1 and 514.7E-2)
- **Shock:** 20 g, 11 ms (pulse sawtooth) in accordance with MIL-STD 810G, Method 516.7 Procedure 1
- For shock/vibe of antennas (such as Model 8230s), refer to ..\CustomerServiceAssistance.pdf
- Refer also to: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\VersaSync and VersaPNT>

VersaSyncs/VersaPNTs have been shock/vibe tested against MIL-STD-810F/MIL-STD-810G

- Refer to the VersaSync/VersaPNT online user guides/datasheets for specs.

VersaSync Evaluation kits (VEK)

Note: Breakout cables are not included with the purchase of base VersaSync. They are included with purchase of optional VersaSync Evaluation Kit (VEK).

Two different VEK kits available

1. VersaSync Evaluation Kit (with L1 antenna for non-SAASM)

- Refer to “A)” further below

2. VersaSync Evaluation Kit (VEK) with L1/L2 Antenna (SAASM)

- Refer to “B)” further below

Common cables included with both kits (such as all breakout cables)

- Refer to “C)” further below

A) VersaSync Evaluation Kit (with L1 antenna, for non-SAASM)



Associated Documentation

- **NON-SAASM VEK Process Detail (1228-0000-0702-PD) in Arena:**
<https://files.bom.com/download/aMObbS94syYvzTbtHgw0vwLhcaa6nJNn/iltapwihvxcxclvpejvrfmexsyzdloqv/1228-0000-0705-PD%20Rev%201.pdf>

Details of the VersaSync Eval Kit (Non-SAASM)

- **P/N for the kit: 1228-0000-0702** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1225990093&version_id=10625293458)
- Includes Carrying Case, breakout cables, L1 antenna

1228-0000-0702 In Production		
VersaSync Evaluation Kit		
Revision: >3 - In Production Effective as of 01/12/2017 10:17:13 AM, Unshared		
Specs Bill of Materials Where Used Sourcing Costing Files Compliance Revisions Notifications		
Indented Sourcing Flat Costing Purchasing Custom Redline Compare Lookup		
Contains 12 first-level Items, 60 line Items, 49 unique Items, 1 of which is shared.		
#	Item Number	Item Name
1	1222-0001-0600 rev 3 P	8230 Antenna
2	1228-0000-0702-PD rev 2 P	VersaSync Evaluation Kit Process Detail
3	1228-5000-0051 rev 6 P	VersaSync Getting Started Guide
4	CA01R-ONSA-D016 rev 3 P	CABLE ASSEMBLY, SMA MALE, N MALE, 5METER - 16FEET
5	CA06R-EUC7-0001 rev 1 P	AC CORD,EU to C7, 2.5A, 250V, 79C
6	CA06R-N1C7-0001 rev 2 P	North American 3Amp Class II Cordset w/C7 Connector, Unpolarized
7	CA08R-3M00-0001 rev 2 P	CABLE, 20 PIN PLUG TO MULTIPLE CONNECTOR, 1FT, TYPE 1, VEK
8	CA08R-CRET-0002 rev 3 P	CABLE, 16 PIN CIRC MALE TO RJ45 FEMALE, 16 IN, VEK
9	CA08R-CRPB-0002 rev 4 P	CABLE, 5 PIN CIRC MALE TO 2.1MM POWER RECEPTACLE, 1FT, VEK
10	CA08R-CRUB-0002 rev 5 P	CABLE, 26 PIN CIRC MALE TO 20 PIN PLUG AND USB TYPE B FEMALE, 1FT, VEK
11	MP01R-0004-2400 rev 2 P	Carrying Case, 900 ci.
12	PS06R-2201-DT03 rev 2 P	Power Supply, Desktop, 100 to 240 VAC, 12VDC, 2.5A

CA01R-ONSA-D016 (Antenna cable)

CA08R-3M00-0001 (I/O Breakout cable)

CA08R-CRET-0002 (Ethernet breakout cable)

CA08R-CRUB-0002 (I/O cable)

Certification of the breakout cables

Q Are the eval kit cables built by Orolia utilizing an aircraft certified classification so these can be used airborne (or are they round testing/reference only)?

A (per Ron Dries ~4 Apr 2019) The cables are not certified for aircraft. They are for lab integration.

Q For the Power and Ethernet ODU connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

B) VersaSync Evaluation Kit (VEK) with L1/L2 Antenna (SAASM)



Note: Breakout cables are not included with the purchase of base VersaSync. They are included with purchase of optional VersaSync Evaluation Kit (VEK).

Associated Documentation

- **SAASM VEK Process Detail (1228-0000-0705-PD) in Arena:** https://app.bom.com/items/detail-spec?item_id=1252116150&version_id=11081094198&orb_msg_single_search_p=1

Details of the VersaSync Eval Kit (SAASM)

- **P/N for the SAASM kit: 1228-0000-0705** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1251725771&version_id=11073925168)
- Includes Carrying Case, breakout cables, L1/L2 antenna (Model 8225S, P/N 1184-0001-0600) power supply. Sample BOM below (always verify it's still current)

#	Item Number	Item Name
1	1184-0001-0600 rev.4	8225S GPS Antenna, L1-L2
2	1228-0000-0705-PD rev.1	Versa Evaluation Kit (VEK) with L1/L2 Antenna Process Detail
3	1228-5000-0051 rev.5	VersaSync Evaluation Kit Quick Reference Guide
4	CA01R-ONSA-D016 rev.2	CABLE ASSEMBLY, SMA MALE, N MALE, SMETER - 16FEET
5	CA08R-EUC7-0001 rev.1	AC CORD, EU to C7, 2.5A, 250V 70C
6	CA08R-N1C7-0001 rev.2	North American 3Amp Class II Cordset w/C7 Connector, Unpolarized
7	CA08R-3M00-0001 rev.2	CABLE, 20 PIN PLUG TO MULTIPLE CONNECTOR, 1FT, TYPE 1, VEK
8	CA08R-CRET-0002 rev.3	CABLE, 16 PIN CIRC MALE TO RJ45 FEMALE, 16 IN, VEK
9	CA08R-CRUB-0002 rev.3	CABLE, 8 PIN CIRC MALE TO 8 PIN PLUG, 1 FT, w/ZEROIZE AND SAASM CON
10	CA08R-CRPS-0002 rev.4	CABLE, 5 PIN CIRC MALE TO 2.1MM POWER RECEPTACLE, 1FT, VEK
11	CA08R-CRUB-0002 rev.4	CABLE, 26 PIN CIRC MALE TO 20 PIN PLUG AND USB TYPE B FEMALE, 1FT, VE
12	MP018-0004-2400 rev.2	Carrying Case, 900 ci.
13	PS068-2200-0703 rev.2	Power Supply, Desktop, 100 to 240 VAC, 12VDC, 2.5A

CA01R-ONSA-D016 (Antenna cable)

CA08R-CRUB-0002 (I/O cable)

CA08R-3M00-0001 (I/O Breakout cable)

CA08R-CRET-0002 (Ethernet breakout cable)

Certification of the breakout cables

Q Are the eval kit cables built by Orolia utilizing an aircraft certified classification so these can be used airborne (or are they round testing/reference only)?

A (per Ron Dries ~4 Apr 2019) The cables are not certified for aircraft. They are for lab integration.

Q For the Power and Ethernet ODU connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

C) Common cables in both Eval kits (such as all breakout cables)

- Refer to (in the online VersaSync user guide, excerpt below)
<http://manuals.spectracom.com/VSS/Content/VSS/SETUP/ToolsCables.htm>

Included Cables

The VersaSync Evaluation Kit contains the following cables (antenna cable not shown):

Power Cable



P/N: CA08R-CRPB-0002



I/O Cable



P/N: CA08R-CRUB-0002



I/O Breakout Cable



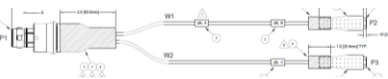
P/N: CA08R-3M00-0001



Ethernet Data Cable



P/N: CA08R-CRET-0002



GNSS Antenna Cable

P/N: CA01R-ONSA-D016 (16ft long)

VersaSync/VersaPNT Options

A) VP-OPT-BSH: Versa Family Interference Detection Suite option

- Refer to the BroadShield datasheet on our website: <https://www.rolia.com/product/broadshield/>
- Refer to VersaSync IDM suite on our site: <https://www.rolia.com/solution/interference-detection-and-mitigation/>
- Refer to the online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/TIME/Broadshield.htm?Highlight=interference%20detection
- Formally known as “Broadshield versa Option”
 - Refer to ECO-2323 for name change (in Arena): https://app.bom.com/changes/detail-approvals?change_id=2398985633
 - **Description:** Change name/description of Versa BroadShield option to Versa Family Interference Detection Suite option

Note: the vast majority of the following Broadshield info is a copy/paste from SecureSync Assist doc, and may vary for VersaSync/VersaPNTs

Links/shortcuts

[Link to press release on a web page](#)

[Link to SecureSync with Broadshield information page](#)

ptp

Link to datasheet on our site: https://spectracom.com/sites/default/files/document-files/SecureSync_BroadShield_Option_revA.pdf

Link to salesforce (pricing/ordering): <https://na28.salesforce.com/01t1A0000056HWv?srPos=0&srKp=01t>


Link to info about Broadshield in online SecureSync manual:

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.

BROADSHIELD™ from **TALEN-X**
COMBINED BY SPECTRACOM & TALEN-X

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



The diagram shows a hardware unit with a GPS/GNSS antenna and a rack-mounted server. A hand icon with a signal symbol is labeled 'GPS/GNSS'.

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)

VersaSync Software changes associated w/BroadShield (descending order)

pseudod: new daemon created to pass ublox messages to the Broadshield option

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**.

broadschild.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=broadschild

broadschild.ini file

path to the broadschild.ini file: home/spectracom/config/Talen-X/BroadShield.ini

“Talen-X/BroadShield.ini: Permission denied”

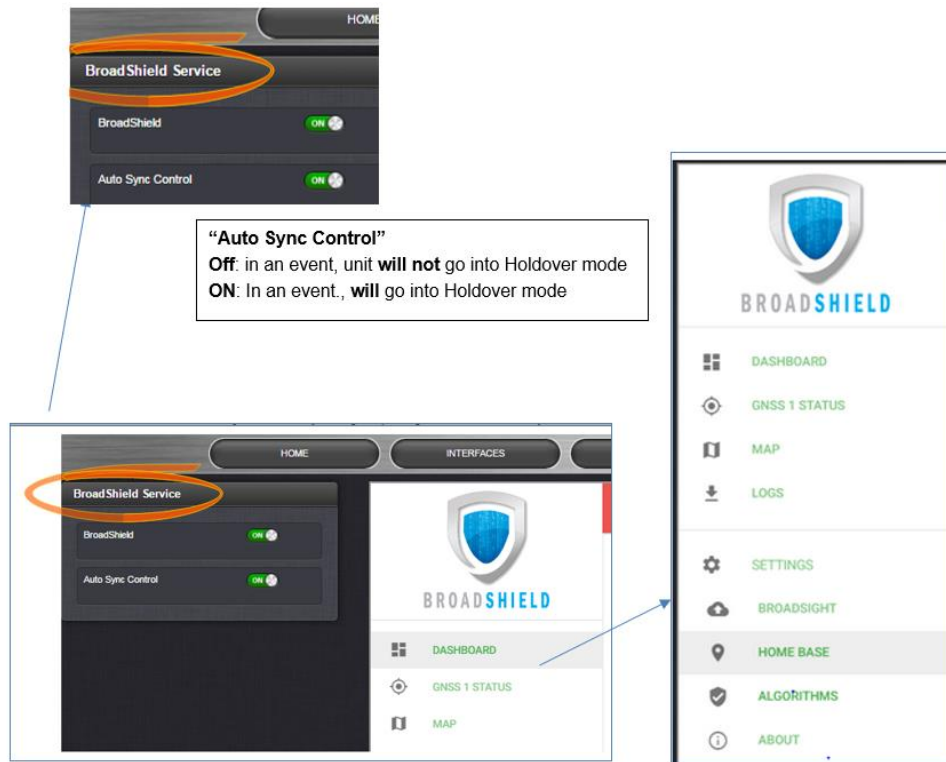
- refer to Salesforce case 172828

default state after installing license: Broadshield is **disabled** after adding license file

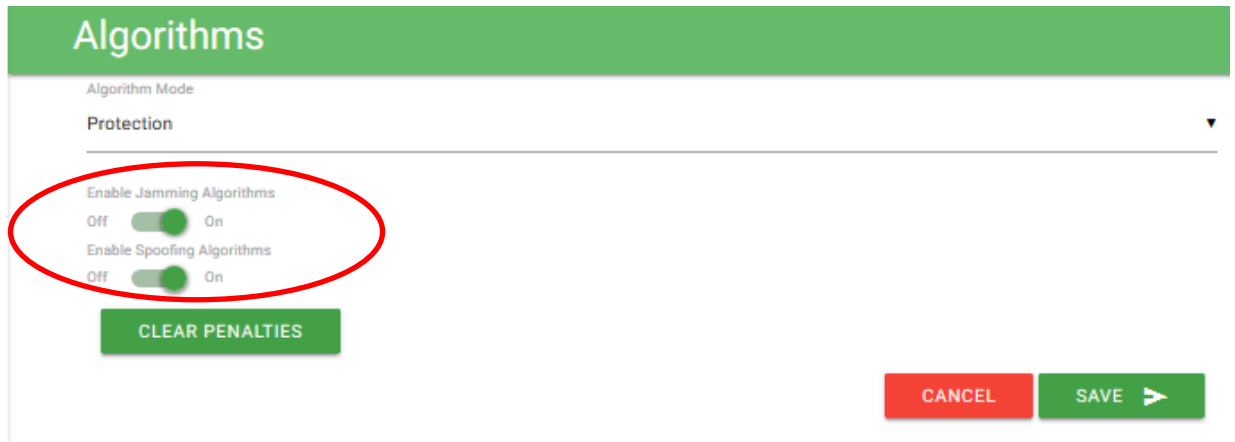
A) To configure the mode of operation

1. Navigate to **MONITORING > BroadShield**.
2. In the BroadShield Service panel on the left, configure the desired setting:

Note: Turning BroadShield OFF and Auto Sync Control ON is an invalid setting and will cause a "Failed to connect to the unit..." error.

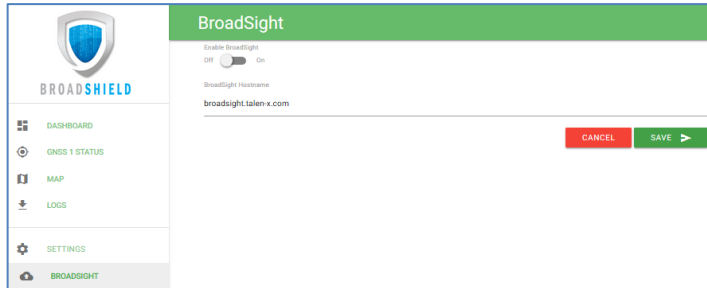


3. In the BroadShield Web UI on the right, navigate to **SETTINGS** > **ALGORITHMS**, and ensure that Jamming and/or Spoofing detection slider switches are enabled.

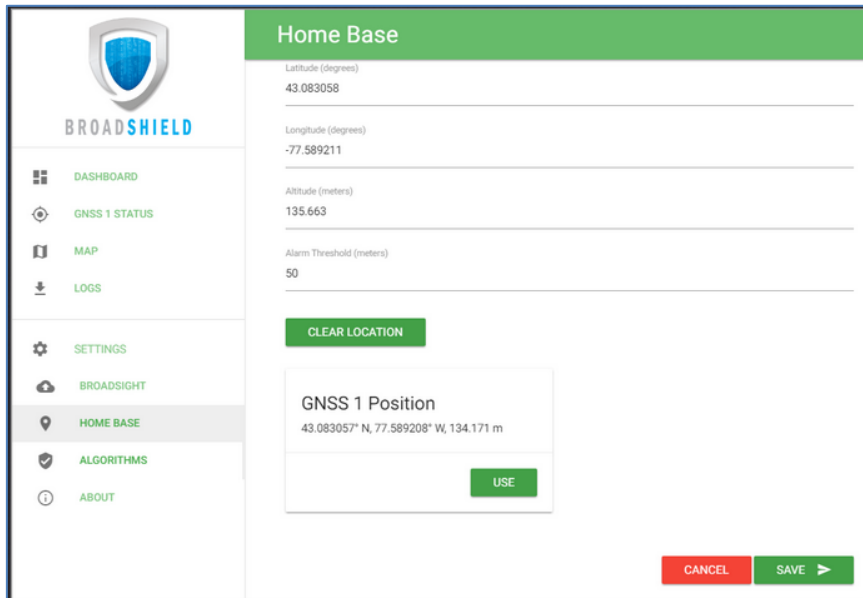


B) BroadSight

- BroadSight is a service that allows collection of data from multiple BroadShield units and provides a dashboard view of the data.
- “BroadSight for VersaSync is currently not supported”/“BroadSight for VersaPNT is currently not supported” (note from User Guides, Nov 2019)



C) “Home Base” position (optional)



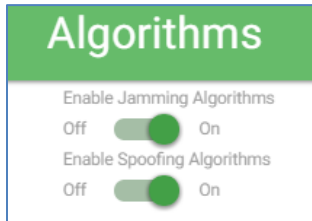
- By setting the HOME BASE position you allow BroadShield to use this location as a reference position for spoofing detection:
 - Should BroadShield detect that the geographic position reported by SecureSync's GPS receiver seems to move beyond the set Alarm Threshold (even though SecureSync does not 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 SAVE 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.

D) Algorithms (“Enable Jamming Algorithms” / “Enable Spoofing Algorithms”)



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.

E) About

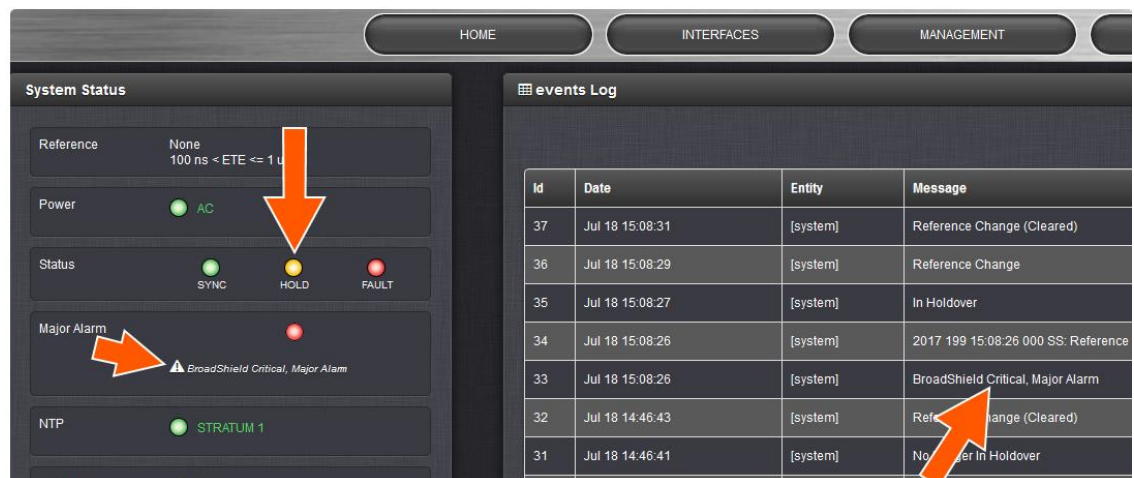
- Displays Version and Build Date of the BroadShield software.

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

If BroadShield detects a jamming or spoofing event, SecureSync will:

- emit 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).

A screenshot of the BroadShield web UI. The top navigation bar includes "HOME", "INTERFACES", and "MANAGEMENT". The main content is split into two panels. The left panel, titled "System Status", shows various system metrics: Reference (None), Power (AC), Status (SYNC, HOLD, FAULT), Major Alarm (BroadShield Critical, Major Alarm), NTP (STRATUM 1), and Oscillator (47.0°C). The right panel, titled "events Log", displays a table of events. An orange arrow points from the "Major Alarm" status in the System Status panel to the corresponding entry in the Events Log table. Another orange arrow points from the "BroadShield Critical, Major Alarm" entry in the Events Log table to the "Major Alarm" status in the System Status panel.

Id	Date	Entity	Message
37	Jul 18 15:08:31	[system]	Reference Change (Cleared)
36	Jul 18 15:08:29	[system]	Reference Change
35	Jul 18 15:08:27	[system]	In Holdover
34	Jul 18 15:08:26	[system]	2017 199 15:08:26 000 SS: Reference
33	Jul 18 15:08:26	[system]	BroadShield Critical, Major Alarm
32	Jul 18 14:46:43	[system]	Reference Change (Cleared)
31	Jul 18 14:46:41	[system]	No longer In Holdover

Available Broadshield notifications

Management -> Notifications page of the browser



Real-time monitoring via 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.)

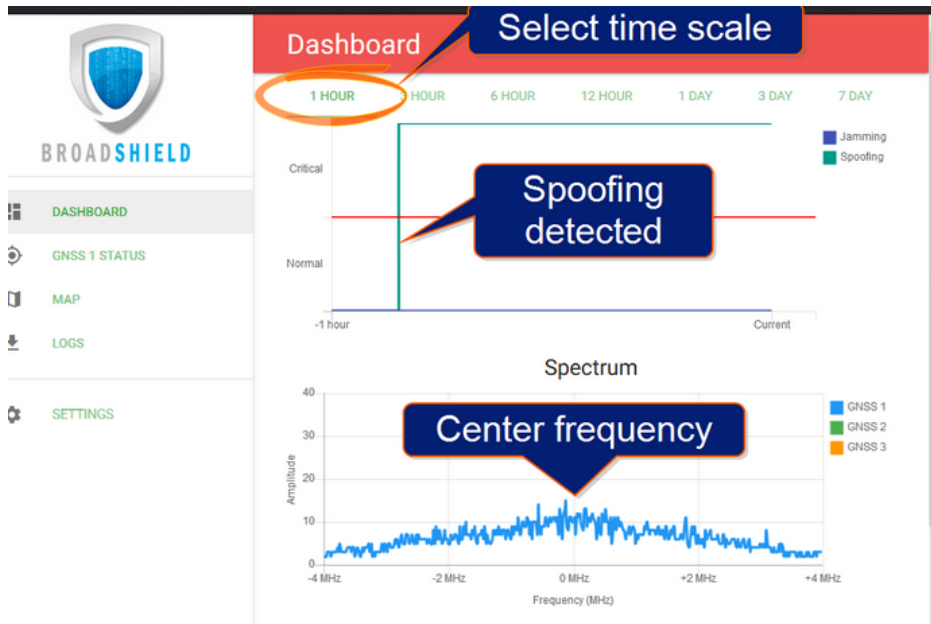
The embedded Broadshield Web UI will open, displaying the Dashboard and providing access to the following panels:

DASHBOARD:

- 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;

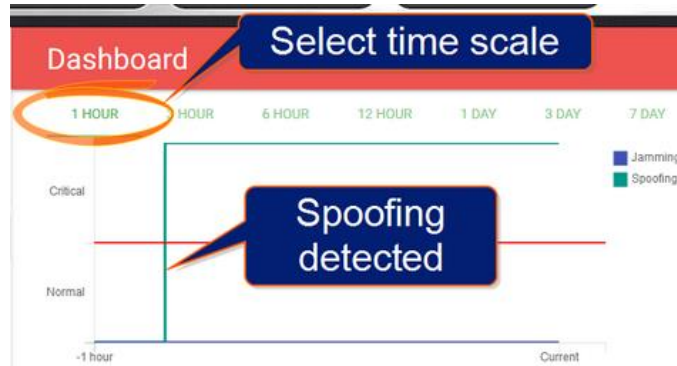
green = no alarms at this time



F) Top graph of the dashboard (displays past signal level over time)

Note:

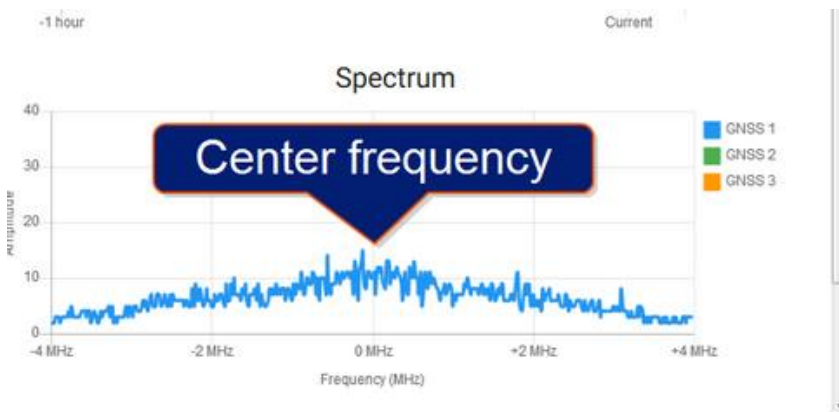
- You can **change the time scale** by clicking on any of the labels at the top (between “1 hour” and “7 days”)



- 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.)

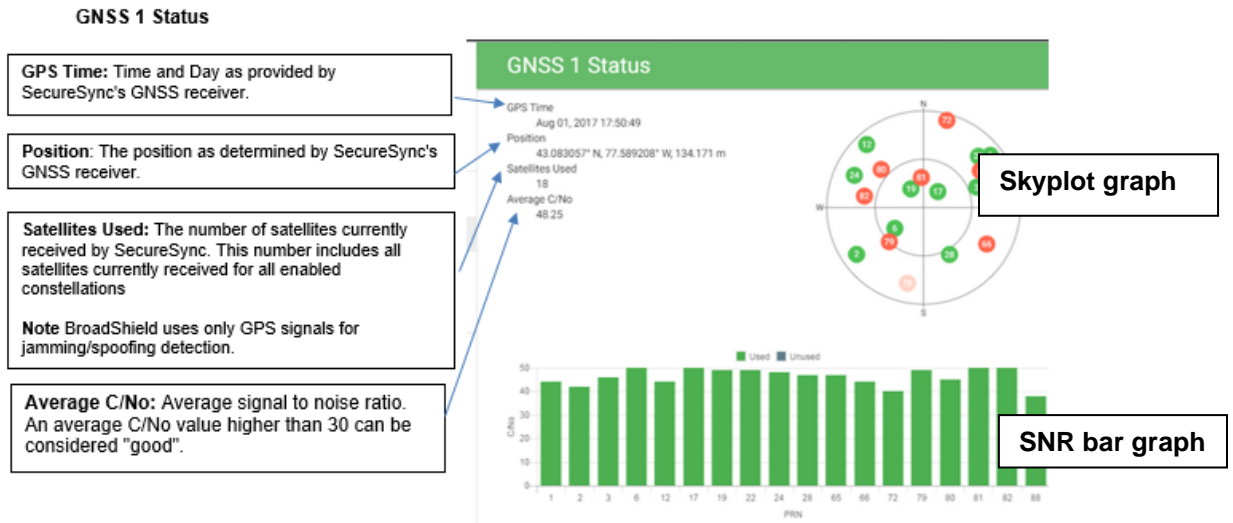
G) Bottom graph of the dashboard (labeled “Spectrum”) (shows current signal over the GPS band)



- 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).



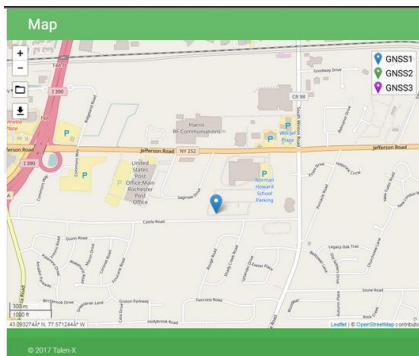
The center of the skyplot represents the antenna position. The skyplot shows all GPS satellites currently being tracked and – if enabled (under INTERFACES: REFERENCES > GNSS Reference: GNSS 0 > Edit button > Selected Constellations) – will also display all GLONASS satellites (numbered 65 and higher). 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)

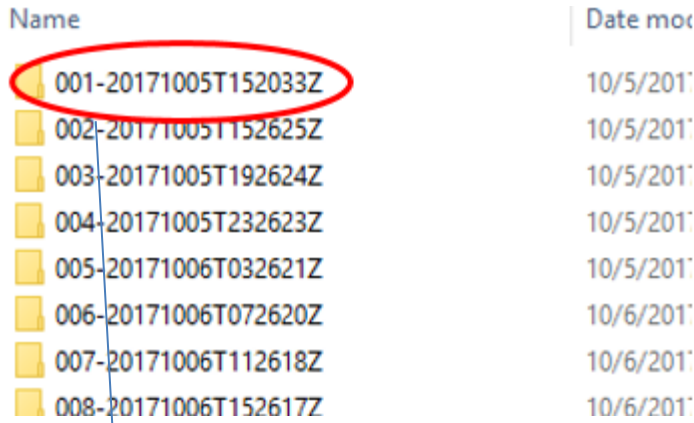
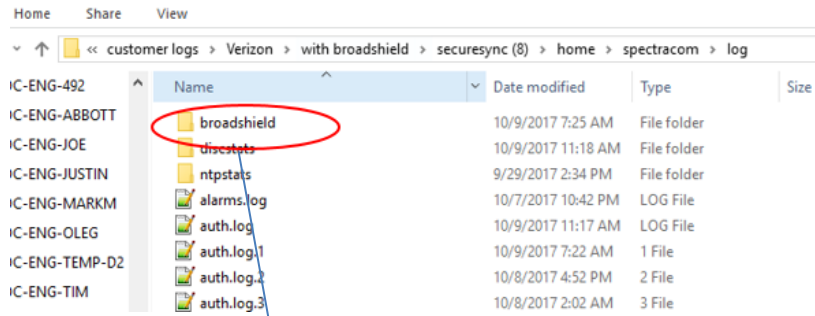


Note: the map data is not part of the BroadShield software, but is downloaded from the Internet. Hence, this feature is only available if your SecureSync unit is connected to the Internet.

- 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)

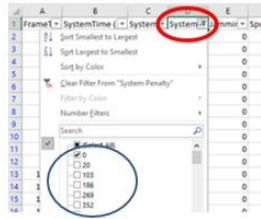
Home -> Spectracom -> Log -> BroadShield directory



Example SystemStatus.csv file:

A	B	C	D	E	F	G	H	I
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

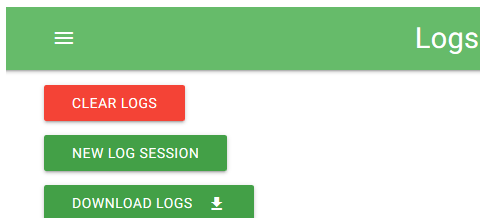
Jamming Penalties

Spoofing Penalties

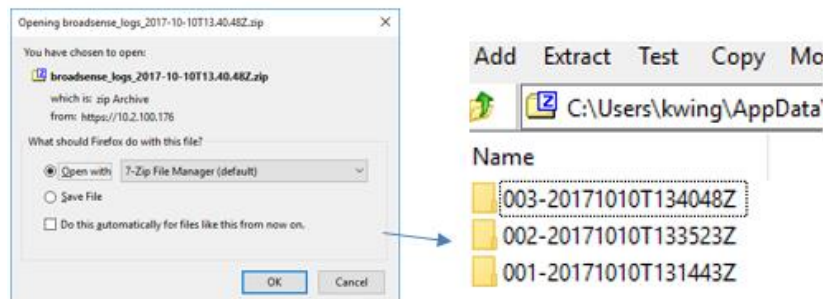
Rotation of BroadShield’s log (SystemStatus.csv files)

- Per Paul M (9 Oct 17) If CF card usage is greater than 70%, Broadshield logs are deleted.

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 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
Oct 5 15:26:25 ohcntp2 ohcntp2: [system] BroadShield Critical, Major, Cleared
Oct 8 02:41:02 ohcntp2 ohcntp2: [system] BroadShield Critical, Major Alarm
Oct 8 02:41:02 ohcntp2 ohcntp2: [system] In Holdover
Oct 8 02:41:02 ohcntp2 ohcntp2: [system] 2017 281 02:41:02 000 SS: Reference changed to Time Ref: none
PPS Ref: none
Oct 8 02:41:03 ohcntp2 ohcntp2: [system] Reference Change
Oct 8 02:41:04 ohcntp2 ohcntp2: [system] Reference Change (Cleared)
Oct 8 02:42:05 ohcntp2 ohcntp2: [system] BroadShield Critical, Major, Cleared
Oct 8 02:42:06 ohcntp2 ohcntp2: [system] Reference Change
Oct 8 02:42:06 ohcntp2 ohcntp2: [system] 2017 281 02:42:06 000 SS: Reference changed to Time Ref: gps0
PPS Ref: gps0
Oct 8 02:42:07 ohcntp2 ohcntp2: [system] No Longer In Holdover
Oct 8 02:42:08 ohcntp2 ohcntp2: [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 ohcntp2 ohcntp2: [system] 2017 278 07:00:46 000 XO: Ref Changed: old=gps0 new=none
Oct 5 07:00:46 ohcntp2 ohcntp2: [system] 2017 278 07:00:46 000 XO: Phase Reference Invalid.
Oct 5 07:00:48 ohcntp2 ohcntp2: [system] 2017 278 07:00:47 000 XOS: Rb track off -- free run
Oct 5 07:00:54 ohcntp2 ohcntp2: [system] 2017 278 07:00:54 000 XO: Ref Changed: old=none new=gps0
Oct 5 07:00:54 ohcntp2 ohcntp2: [system] 2017 278 07:00:54 000 XO: Phase Reference Valid.
Oct 5 07:02:28 ohcntp2 ohcntp2: [system] 2017 278 07:02:28 000 XOS: Rb synchronized
Oct 5 07:03:00 ohcntp2 ohcntp2: [system] 2017 278 07:03:00 000 XOS: Frequency error recalculated: -00.000023
(-2.337x10^-12)
Oct 5 07:31:31 ohcntp2 ohcntp2: [system] 2017 278 07:31:31 000 XO: Ref Changed: old=gps0 new=none
Oct 5 07:31:31 ohcntp2 ohcntp2: [system] 2017 278 07:31:31 000 XO: Phase Reference Invalid.
Oct 5 07:31:32 ohcntp2 ohcntp2: [system] 2017 278 07:31:32 000 XOS: Rb track off -- free run
Oct 5 07:31:39 ohcntp2 ohcntp2: [system] 2017 278 07:31:39 000 XO: Ref Changed: old=none new=gps0
Oct 5 07:31:39 ohcntp2 ohcntp2: [system] 2017 278 07:31:39 000 XO: Phase Reference Valid.
Oct 5 07:33:14 ohcntp2 ohcntp2: [system] 2017 278 07:33:13 000 XOS: Rb synchronized
```

```
Oct 5 10:21:08 ohcntp2 ohcntp2: [system] 2017 278 10:21:07 000 XOS: Frequency error recalculated: -00.000011
```

(-1.192x10⁻¹²)
 Oct 5 11:02:10 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:02:10 000 XO: Ref Changed: old=gps0 new=none
 Oct 5 11:02:10 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:02:10 000 XO: Phase Reference Invalid.
 Oct 5 11:02:12 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:02:11 000 XOS: Rb track off -- free run
 Oct 5 11:02:15 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:02:15 000 XO: Ref Changed: old=none new=gps0
 Oct 5 11:02:15 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:02:15 000 XO: Phase Reference Valid.
 Oct 5 11:03:49 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:03:49 000 XOS: Rb synchronized
 Oct 5 11:04:05 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:04:04 000 XOS: Frequency error recalculated: 00.000059
 (5.980x10⁻¹²)
 Oct 5 11:23:09 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:09 000 XO: Ref Changed: old=gps0 new=none
 Oct 5 11:23:09 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:09 000 XO: Phase Reference Invalid.
 Oct 5 11:23:11 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:10 000 XOS: Rb track off -- free run
 Oct 5 11:23:13 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:13 000 XO: Ref Changed: old=none new=gps0
 Oct 5 11:23:13 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:13 000 XO: Phase Reference Valid.
 Oct 5 11:23:15 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:15 000 XO: Ref Changed: old=gps0 new=none
 Oct 5 11:23:15 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:15 000 XO: Phase Reference Invalid.
 Oct 5 11:23:17 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:17 000 XO: Ref Changed: old=none new=gps0
 Oct 5 11:23:17 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:23:17 000 XO: Phase Reference Valid.
 Oct 5 11:24:52 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:24:51 000 XOS: Rb synchronized
 Oct 5 11:25:25 ohcnntpz2 ohcnntpz2: [system] 2017 278 11:25:24 000 XOS: Frequency error recalculated: -00.000024
 (-2.483x10⁻¹²)
 Oct 5 12:01:16 ohcnntpz2 ohcnntpz2: [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 ohcnntpz2 ohcnntpz2: [system] 2017 281 00:47:09 000 XOS: Frequency error recalculated: -00.000006
 (-6.704x10⁻¹³)
 Oct 8 02:41:03 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:41:03 000 XO: Ref Changed: old=gps0 new=none
 Oct 8 02:41:03 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:41:03 000 XO: Phase Reference Invalid.
 Oct 8 02:41:04 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:41:04 000 XOS: Rb track off -- free run

Event ended
 Oct 8 02:42:07 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:42:07 000 XO: Ref Changed: old=none new=gps0
 Oct 8 02:42:08 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:42:07 000 XO: Phase Reference Valid.
 Oct 8 02:43:42 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:43:41 000 XOS: Rb synchronized
 Oct 8 02:43:49 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:43:48 000 XOS: Frequency error recalculated: -00.000002
 (-2.917x10⁻¹³)
 Oct 8 05:50:56 ohcnntpz2 ohcnntpz2: [system] 2017 281 05:50:55 000 XOS: Frequency error recalculated: 00.000005
 (5.366x10⁻¹³)

VersaSync Option Card

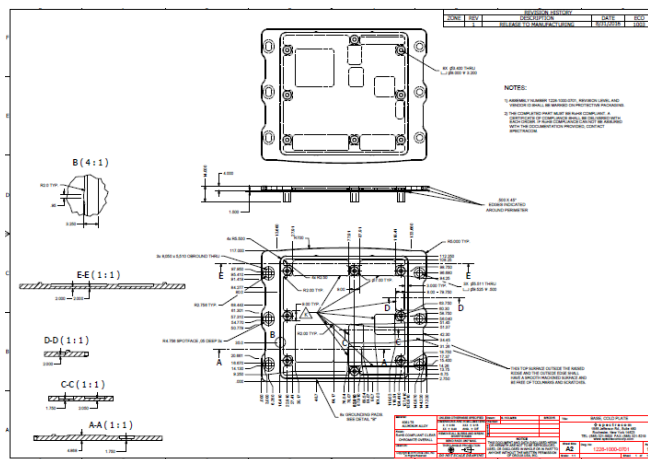
- One Option Card can be installed internally
 - SAASM GPS receiver needs to be installed using an Option Card
- Option Card capability planned to be used for “Specials”

Chassis related / Mounting

***Mounting plate/holes



- Our P/N for the metal base plate: 1228-1000-0701 (in Arena at: https://app.bom.com/items/detail-spec?item_id=1214660528&version_id=10625293338&)
- Drawing of mounting plate (1228-1000-0701, available as PDF or zip) in Arena at: https://app.bom.com/items/detail-attach?item_id=1214660528&version_id=10625293338 (similar to the drawing below):



(1226-1000-9701) metal plate on bottom of chassis

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

(1226-1000-9703) Top Cover

Ruggedization testing (MIL-STD-810G/MIL-STD-461F)

- Ruggedized – tested to:
- MIL-STD-810G (Environment)
- MIL-STD-461F (EMC)

RUGGED, LOW SWAP FORM FACTOR

VITA75 form factor
147.3 x 127.5 x 63.0mm
0.91 kg (2.0 lbs.)
Power (10-32 VDC) : 10-12W*
Ruggedized – tested to:
MIL-STD-810G (Environment)
MIL-STD-461F (EMC)



Designed for reliability and easy maintenance

* Depending on hardware component configuration.

PNT Principles | 6/6/2018

106 orolix

IP64 rating/IP65 Plugs for VersaSync SAASM and SMA holes

- Refer to ECO-FAI-1637 (in Arena): https://app.bom.com/changes/detail-summary?change_id=2393362653&
- P/Ns:
 - **MP11-0004-0003** (SAASM plug)
 - **MP11-0004-0004** (SMA hole plug)

ECO-2006 (Changes to Cover and Base For Profen Order - IP65 Sealing Issues) (~Feb 2019)

- In Arena at: https://app.bom.com/changes/detail-affected?change_id=2396154865

VersaSync/VersaPNT Model Numbering scheme

Model 1228- A B C D

A is Chassis configuraton

- 0= (1) 10 MHz output
- 1= (4) 10 MHz outputs
- 2= (4) 10 MHz outputs (see Note further below)
- 3= (3) 10 MHz outputs

B is Oscillator

- 1= Standard OCXO (5PPB)
- 2= CSAC
- 4= Low Phase Noise OCXO (1PPB)

C is GPS/GNSS receiver

- 1= uBlox GNSS receiver (commercial receiver)
- 2= SAASM GPS receiver (L1/L2)

D is whether Option Card is installed

- 0= Option Card not installed
- 1= SAASM GPS receiver installed (note that SAASM receiver requires an Option Card be installed)
- 4=IRIG AM In/Out Option Card installed

Note about Table A (above) having two values ("1" and "2") for 4x10 MHz outputs

Per Ron Dries (4 Oct 2021) The "2" for chassis configuration was originally because IRIG AM was going to take up 3 of the 5 SMA's on the front, leaving 1 for 10MHz and 1 for the GNSS antenna. However, the IRIG AM design changed and it is now going through the configurable I/O.

From Engineering:

"the 1228-2xxx was meant to indicate that while there were still five SMAs only one would be available for 10MHz has opposed to four in the 1228-1xxx configuration.

After the model numbers had been solidified though the design changed so that the IRIG-AM signals went through the IO connector instead of the SMAs and so it was back to four 10MHz's."

For edit purposes

A is Chassis configuraton

- 0= (1) 10 MHz output
- 1= (4) 10 MHz outputs
- 2= (4) 10 MHz outputs (see Note further below)
- 3= (3) 10 MHz outputs

B is Oscillator

- 1= Standard OCXO (5PPB)
- 2= CSAC
- 4= Low Phase Noise OCXO (1PPB)

C is GPS/GNSS receiver

- 1= uBlox GNSS receiver (commercial receiver)
- 2= SAASM GPS receiver (L1/L2)

D is whether Option Card is installed

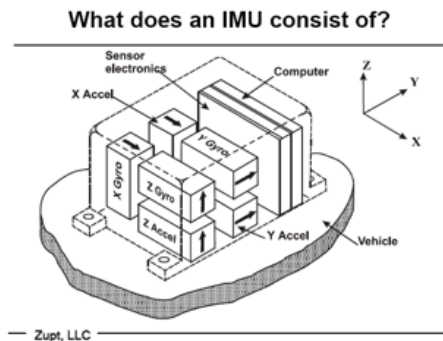
- 0= Option Card not installed
- 1= SAASM GPS receiver installed (note that SAASM receiver requires an Option Card be installed)
- 4=IRIG AM In/Out Option Card installed

Example Standard VersaSync configurations/Model Numbering scheme

VersaSync Model	10Mhz out, Qty	Oscillator	GNSS receiver	Option Card
1228-0110	1	OCXO	GNSS L1	
1228-0410	1	High Perf OCXO	GNSS L1	
1228-1110	4	OCXO	GNSS L1	
1228-1410	4	High Perf OCXO	GNSS L1	
1228-0211	1	CSAC	GNSS L1	
1228-0121	1	OCXO	SAASM GPS L1/L2	
1228-0221	1	CSAC	SAASM GPS L1/L2	
1228-2114	4			IRIG AM input/outputs)

Inertial navigation/IMU (Inertial Measurement Unit) for VersaPNTs

IMU –INERTIAL MEASUREMENT UNIT



3 ACCELEROMETERS

- x, y, z

3 GYROS

- pitch, roll, yaw

6DOF

$\Delta V, \Delta \theta$ OUTPUTS

INS = Inertial Navigation System

IMU + Clock + Processing => position, velocity, attitude

Inertial Navigation

INERTIAL NAVIGATION Need GPS to provide initial velocity, v_0 , and position, p_0

$$\vec{v} = \int \vec{a} \cdot dt + \vec{v}_0 \quad \vec{p} = \int \vec{v} \cdot dt + \vec{p}_0$$

- Measure \vec{a} ; integrate twice; determine position over time
- Know where you started, know where you are now
- No external signals or references
- Cannot be jammed or spoofed
- Position Errors grow with time exponentially
- Double integration
- GNSS Denied Environment
- Holdover Oscillator => Time
- IMU => Position

PNT Principles | 6/6/2018 64 orolیا

ATTITUDE

- Angular measurement: θ
- Gyro measures angular increments: $\delta\theta$
- Same approach
- Initial angle = known
- North & Up alignment
- Integrate changes over time
- Up aligns with gravity field
- North aligns with earth rotation

$$\theta = \int \Delta \theta \cdot dt + \theta_0$$

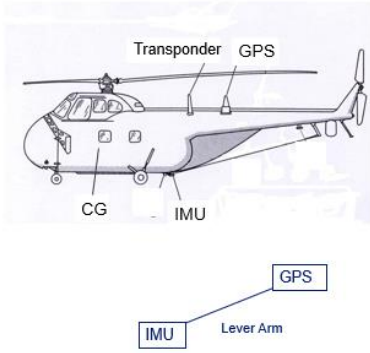
Figure 5-1 The axis of rotation.

PNT Principles | 6/6/2018 65 orolیا

Lever Arm

LEVER ARM

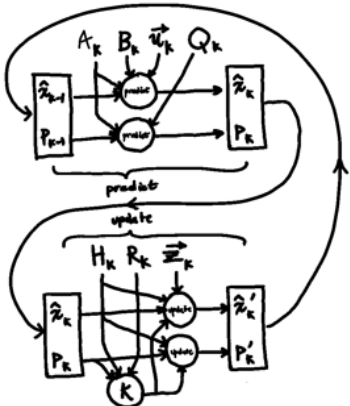
- Several different points of interest for tracking an aircraft
- Tracking precision (~1m) is finer than size of aircraft (~10m)
- "Lever Arm" is the spacing between these points
- Tracking calculations must account for this separation in 3 dimensions: x, y, z



PNT Principles | 6/6/2018 66 orolida

Kalman Filter

OPTIMAL ESTIMATION – THE KALMAN FILTER



IF

- Have an analytical model for the behavior of your system – for example: the trajectory of an aircraft

AND

- Know the statistical error behavior of your measurements

THEN

- You can make a very good estimate of the true position by filtering the measurements and combining the them in an optimal way over time to obtain a composite solution

PNT Principles | 6/6/2018 69 orolida

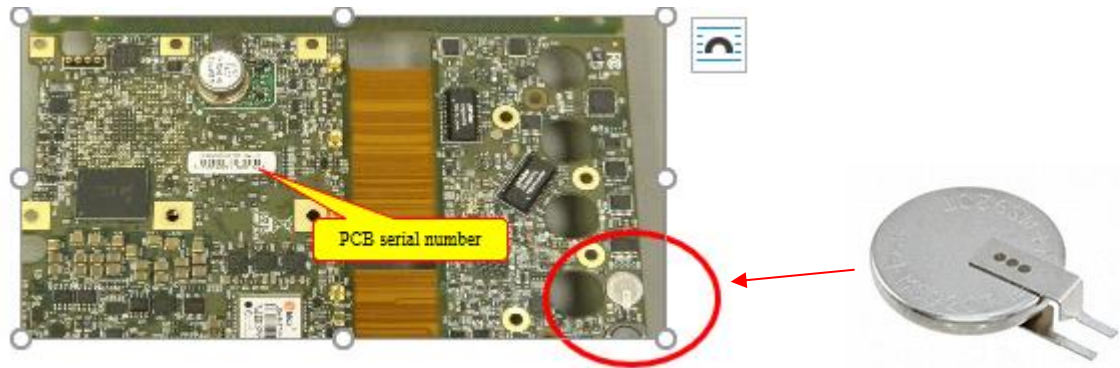
Real Time Clock (RTC) and RTC rechargeable Lithium battery (BT1)

A) Real Rime Clock (RTC)

Slightly edited Email from Emmanuel (Sept 2016) I confirm that VersaSync embeds a real time clock which ensures that Time of Day is maintained even when the clock is shut down.

So, behaviour 3 [The current time (internally counted from the moment the unit was turned off)] will be observed when the unit is powered on (after a few 10s seconds of initialization). Note however that only Time of Day (hour, minute, second, date) are maintained. The 1 pps will not be accurate to UTC until disciplining (to GPS or any other reference) is effective.

B) 3vdc rechargeable Lithium battery for RTC ("BT1") (one installed in every VersaSync/PNT)

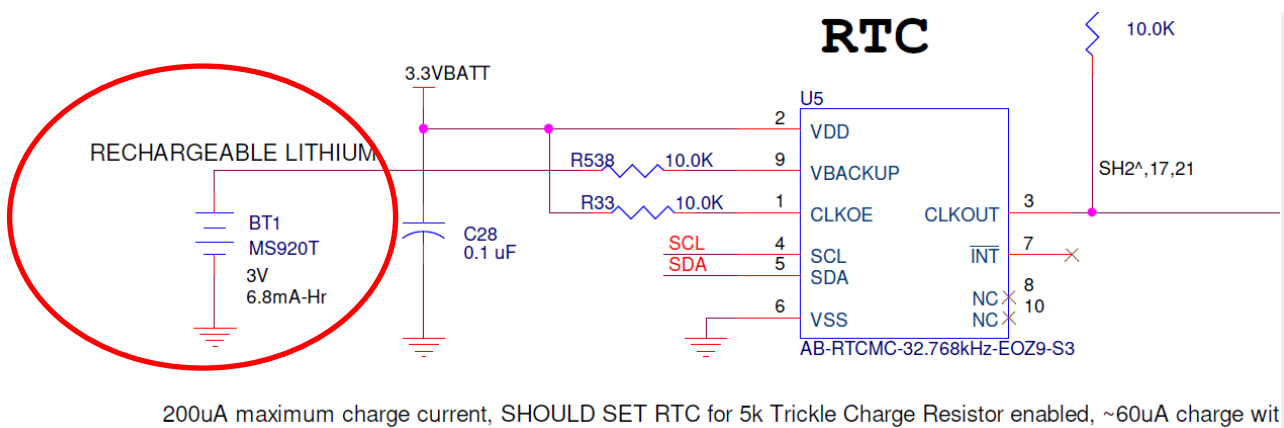


➤ **Description:** "BATT LITH 3V 6.5MAH COIN 9.5MM"

Part Numbers for this 3v Lithium battery

- **Seiko Instruments P/N: MS920T** <https://www.sii.co.jp/en/me/datasheets/ms-rechargeable/ms920t/>
- **Digikey P/N: 728-1077-ND** <https://www.digikey.com/products/en?keywords=728-1077-ND%20>

below is from main board schematic (1228-1001-0200) in Arena: https://app.bom.com/items/detail-spec?item_id=1232721353&version_id=10931615798&orb_msg_single_search_p=1



FAQs about the rechargeable RTC Lithium battery (“*Backup Battery*”)

- Refer to the online Versa user guide (excerpt below) at:
http://manuals.spectracom.com/VSS/Content/VSS/INTRO/Specs_InputPower.htm

“VersaSync has an internal battery to support the Real Time Clock. The battery is a small lithium coin cell that is not customer-replaceable. This battery will keep approximate time and date in a shutdown state over ~135 days before requiring recharge. After full drain, the battery will require ~5 days to fully recharge. Minimum battery life is ~30+ years.”

1) Expected life expectancy of the rechargeable lithium battery

Response from Rachel to Keith (2 Aug 2019, responding to my general questions about batteries in Versas)

“...Since it is rechargeable and holding such a small amount of data, this battery is estimated to not fail or need to be changed at all during the lifetime of the product (I think maybe the worst case scenario is like 30 years based on our calculations). So there are no customer recommendations on that.”

- Refer to the online Versa user guide (excerpt below) at:
http://manuals.spectracom.com/VSS/Content/VSS/INTRO/Specs_InputPower.htm

“VersaSync has an internal battery to support the Real Time Clock. The battery is a small lithium coin cell that is not customer-replaceable. This battery will keep approximate time and date in a shutdown state over ~135 days before requiring recharge. After full drain, the battery will require ~5 days to fully recharge. Minimum battery life is ~30+ years.”

2) Customer Access to battery

Q Does this imply that there is a battery inside the VersaSync?

A (per Ron Dries 4 Apr 2019) there is a battery inside VersaSync for RTC operation when power is removed. The customer has no electrical access to this battery. It is only connected to the RTC chip

- Refer to the online Versa user guide (excerpt below) at:
http://manuals.spectracom.com/VSS/Content/VSS/INTRO/Specs_InputPower.htm

*“VersaSync has an internal battery to support the Real Time Clock. **The battery is a small lithium coin cell that is not customer-replaceable.** This battery will keep approximate time and date in a shutdown state over ~135 days before requiring recharge. After full drain, the battery will require ~5 days to fully recharge. **Minimum battery life is ~30+ years.**”*

3) Flightworthiness of the battery

Q can you provide specification for purposes of flightworthiness analysis?

A (per Ron Dries 4 Apr 2019) The RTC battery is a Seiko MS920T-FL27E. It is a low capacity rechargeable lithium. I do not know what a spec for purposes of flight worthiness is, however, please note that VersaSync can't be used for any flight or safety critical application because it does not meet MIL-STD-704 requirement of operation for 7 seconds with 0V DC input voltage.

Question about batteries Keith sent to Apps (and others)

Regarding VersaSync/PNT literature (such as the online user guide and the VeraSAASMguide 1228-5000-0053), Morgan just fielded a VersaSync customer call regarding if there is/are a battery/batteries in a SAASM option

VersaSync, and if the batteries can be changed, etc.

Due to his call, I started looking to see exactly what info VersaSync/PNT customers are currently provided regarding any batteries installed (non-SAASM and SAASM). So, I simply searched for both "Battery" and "Batteries" in both the online user guide and the SAASM doc for Versas. With no hits on either word, I don't see where we may be currently providing any info to customers pertaining to batteries installed/need to be changed. I even looked at the SAASM PD and didn't see any reference to a battery.

All SecureSyncs have one Lithium battery for the RTC, and SAASM-equipped have a second battery.

- 1) Does this same info also apply to Versas? (is there a battery installed in all, a second installed for SAASM)?
- 2) If there is/are one or two Lithium batteries installed, are they customer-changeable, or require equipment return to the factory?
- 3) What is the recommended interval to change the battery/batteries?
- 4) Are there any externally provided indications of a battery needing to be replaced?

If this info is already battery available to customers, please let me know where it can be found (and my apologies for the email). If it's not already available to customers, can you please consider adding this info to the online user guide, SAASM guide, or even a separate document, if you prefer. Customers do periodically ask us for this type of info (as demonstrated by Morgan's call today). Having this info already available for customers (if it's not already) will be greatly appreciated by all 😊!!

Response from Rachel to Keith (2 Aug 2019) responding to my general questions about batteries in Versas)

Yes, there is a small RTC battery in a VersaSync. There is NOT an additional one in SAASM units. Instead, the SAASM in a VersaSync connects to the BACKUP POWER in case of MAIN POWER failure, if the customer's power cables have anything hooked up to that. Otherwise the SAASM just runs on the same power as the rest of the box.

You're right, there currently really isn't any information about the VersaSync/PNT RTC batteries in the manual. The battery is a very tiny rechargeable Lithium battery that is directly soldered to the board itself. Since it is rechargeable and holding such a small amount of data, this battery is estimated to not fail or need to be changed at all during the lifetime of the product (I think maybe the worst case scenario is like 30 years based on our calculations). So there are no customer recommendations on that.

The only sign that the RTC battery had failed in a VersaSync/VersaPNT (and in the SecureSync 2400 as well) would be that the unit would no longer hold the time during shut down; there are no external indications.

I'll add a section clarifying this stuff into the next version of the manuals (it might take a while- I just renewed the revision!).

Enable Battery Backed Time (time sync immediately upon boot-up)

- Note this info copy/pasted from 2400 SecureSync tech note

Configuration

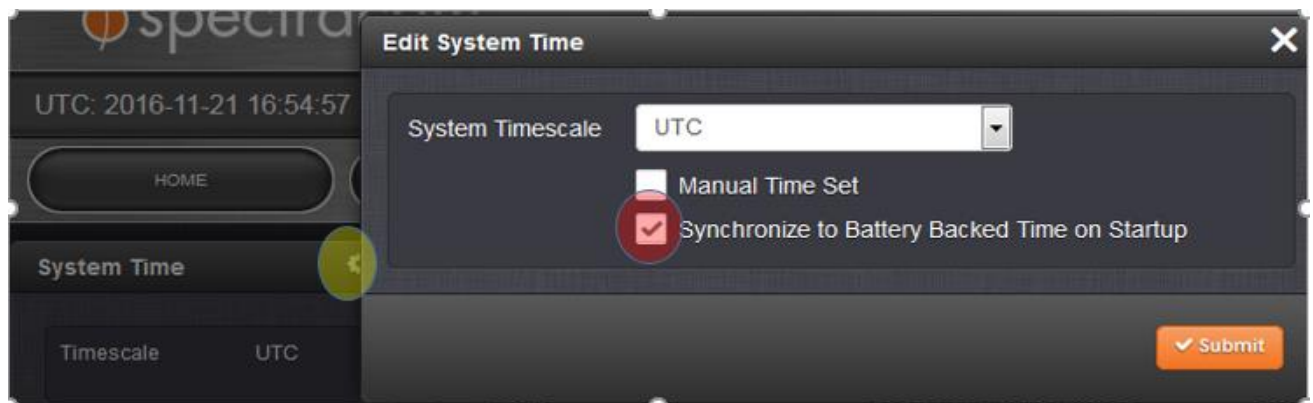
- The button selection is stored in the "rmsf.conf" file (/config directory)

rmsf.conf	Enable battery-backed time button	Startupsync 0: button not selected Startupsync 1: button is selected
-----------	-----------------------------------	---

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)



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.

Optional Standby Mode and Power-up (Vstandby)

Standby Mode

- VersaSync provides a low power mode that keeps the internal oscillator alive for restarting faster after a main supply outage.
- **Standby mode (only the oscillator is powered):** 0.4 W, DC power supply must be within 10.5-12VDC
- Refer to Input power pin-out for info on Vstandby power pin

from Mark McGregor (11 Jul 16): I would like to comment that the Vbat is 10.5V to 12V input voltage range. That may change in the future. I think it is supposed to be called standby power

partial email from Ron Dries (~4 Apr 2019) Vstandby draws about 0.4 watts to keep oscillator, DAC, front panel CPLD running if it is connected but Vmain is not

Post-Boot Sequence, when only Standby power is applied.

partial email from Ron Dries (~4 Apr 2019) Vstandby draws about 0.4 watts to keep oscillator, DAC, front panel CPLD running if it is connected but Vmain is not. **When in standby mode, I believe that the power indicator flashes at a slow rate.**

Confirmation from Mike Pratt with Engineering (17 Oct 2022) Hi Keith, we did confirm recently that the Versa Power LED will slowly pulse when the unit is on standby power only. I think this is not documented yet because standby power is not yet fully implemented as a feature.

The LED should not remain pulsing or blinking after booting up to main power.

Standby Option Cards/Versa configurations with standby power mode implemented and associated Standby Option Cards, per Arena (as of May 2022. Note others may be added)

- **1228-1311:** VersaSync Model 1311 (4x10 MHz, GNSS, mRO + Standby Power Option)
- **1228-1000-0250:** PCB ASSEMBLY, VERSASYNC AM IRIG OPTION CARD W/ STANDBY, GB-GRAM
- **1228-0000-0251:** PCB ASSEMBLY, VERSASYNC mRo OPTION CARD W/ STANDBY, GB-GRAM

Power/Status LEDs

- Refer to online **VersaSync** user guide:
http://manuals.spectracom.com/VSS/Content/VSS/INTRO/Fro_Pa_StatLEDs.htm
- Refer to online **VersaPNT** user guide:
http://manuals.spectracom.com/VSP/Content/VSS/INTRO/Fro_Pa_StatLEDs.htm



LED Lighting Patterns

The table below indicates LED status light patterns for common VersaSync operating statuses.

Common light patterns

Start-up	HEARTB.	OFF	OFF	OFF	OFF	OFF	OFF	OFF
Acquiring fix	FAST	FAST	FAST	FAST	FAST	FAST	HEARTB.	FAST
Software upgrade	FAST	OFF	OFF	FAST	OFF	FAST	HEARTB.	OFF

Adjustable brightness of LEDs

- Starting with version 1.1.5 (~Nov, 2017) brightness of the front panel LEDs is now adjustable. To turn OFF the LEDs, set the brightness to zero.

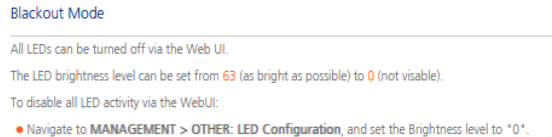
LED Blackout Mode

- All LEDs can be turned off via the Web UI.
- The LED brightness level can be set from **63 (as bright as possible)** to **0 (not visible)**.

To disable all LED activity via the WebUI:

1. Navigate to **MANAGEMENT > OTHER: LED Configuration**
2. Set the Brightness level to **"0"**

Excerpt from the online VersaSync user guide: https://orolia.com/manuals/VSS/Content/VSS/INTRO/Fro_Pa_StatLEDs.htm



LED Lighting Patterns

- The table below indicates LED status light patterns for common Versa operating statuses.

Common light patterns

								
Start-up	HEARTB.	OFF	OFF	OFF	OFF	OFF	OFF	OFF
Acquiring fix	FAST	FAST	FAST	FAST	FAST	FAST	HEARTB.	FAST
Software upgrade	FAST	OFF	OFF	FAST	OFF	FAST	HEARTB.	OFF

Blinking Intervals

The status LEDs can communicate five different operating states:

- "OFF"
- "ON"
- "FAST": blinking interval @ 8Hz
- "SLOW": blinking interval @ 2Hz
- "HEARTBEAT": sinus-shaped interval @ 1Hz

LED Patterns during Boot Sequence

For the first five seconds after power-up all LEDs will be OFF. Then the Power LED will be blinking before it will be lit permanently. If you have configured your unit to operate in Blackout Mode, this will take effect once the blinking cycle ends.

Legend, individual LEDs

Legend for Status LEDs

Icon	Light	Meaning
	OFF	No power
	HEARTBEAT	Booting
	ON	Powered
	OFF	No GNSS reception (0 satellites)
	HEARTBEAT	GNSS acquisition in process (≥ 1 satellite(s), or 1PPS OK, or Time OK)
	SLOW	Jamming detected
	FAST	Antenna short circuit
	ON	GNSS is available as reference (1PPS and Time OK)
	OFF	Inputs not detected/all inputs are disabled
	FAST	1 or more input is missing, or invalid timing on 1 or more input detected
	ON	Inputs are enabled
	OFF	Unit is in Holdover (valid)
	ON	System Clock OK (valid)
	FAST	Invalid Time (Holdover period exceeded, or oscillator damaged)
	OFF	No output signal(s) detected/all outputs are disabled
	FAST	Malfunction detected (short circuit, or overload)
	ON	Outputs are enabled
	OFF	No network detected
	FAST	Network malfunction detected (e.g., no auto-negotiation)
	ON	Network OK, configuration OK
	OFF	Unit OK
	FAST	Unit requires attention; check other status LEDs, see Web UI
	HEARTBEAT	See table LED Lighting Patterns
	OFF	Temperature OK
	FAST	High temperature detected

LED Patterns during Boot Sequence

LED Patterns during Boot Sequence

For the first five seconds after power-up all LEDs will be OFF. Then the Power LED will be blinking before it will be lit permanently. If you have configured your unit to operate in Blackout Mode, this will take effect once the blinking cycle ends.

Post-Boot Sequence, when Standby power is applied.


partial email from Ron Dries (~4 Apr 2019) Vstandby draws about 0.4 watts to keep oscillator, DAC, front panel CPLD running if it is connected but Vmain is not. **When in standby mode, I believe that the power indicator flashes at a slow rate.**



- Confirming note above for Salesforce Case 289597.

Confirmation from Mike Pratt with Engineering (17 Oct 2022) Hi Keith, we did confirm recently that the Versa Power LED will slowly pulse when the unit is on standby power only. I think this is not documented yet because standby power is not yet fully implemented as a feature. The LED should not remain pulsing or blinking after booting up to main power.

Specific examples/notes about the LED indications

1.  Power

Icon	Light	Meaning
	OFF	No power
	HEARTBEAT	Booting
	ON	Powered

	
Start-up	HEARTB.
Acquiring fix	ON
Software upgrade	FAST


LED Patterns during Boot Sequence

For the first five seconds after power-up all LEDs will be OFF. Then the Power LED will be blinking before it will be lit permanently. If you have configured your unit to operate in Blackout Mode, this will take effect once the blinking cycle ends.

2.



(Inputs)

	OFF	Inputs not detected/all inputs are disabled
	FAST	1 or more input is missing, or invalid timing on 1 or more input detected

Inputs LED Blinking fast

Per case 219080, this indicator blinking fast indicates the [Management](#) -> [Reference Priority](#) table has entries for input other references which are not present/valid (example: the LED will flash by factory default, with GPS input applied. By default, this table lists other references besides just GNSS (such as IRIG) which are likely not present. Deleting or at least temporarily unselecting the Enabled checkboxes of all unused/not present references will stop the LED from flashing rapidly.

Email from Keith for Case 219080 (6 Jan 2020) The [Management](#) -> [Reference Priority](#) page of the VersaSync browser lists and prioritizes the available references the VersaSync can sync with (such as GNSS satellites, IRIG input, etc). The LED flashing fast indicates that the VersaSync's Reference Priority table has References listed in this table, which are not currently present/valid.

Not all default entries of various input references in this page of the browser may be used for your particular application. For instance, if the only external input currently being provided to the VersaSync is GNSS 0 (satellites), all other references listed in this table can be optionally either "disabled" or deleted from the table (either just unselect the **"Enabled"** checkbox in that row of the table to keep that entry in the table, or you can delete the entry from the table altogether. Unchecking the "Enabled" checkbox of each reference just alleviates the need to add the entry to the table again, if its ever decided to use this entry in the future. The Enabled checkbox is very handy, especially if you wish to just temporarily disable an input for a short duration, before enabling it again (unchecking the Enable checkbox for GNSS is fairly similar to disconnecting the Antenna cable, to see what happens if GNSS satellites were to be lost, without having to actually touch the antenna cable.

With GNSS (GPS) being the only input reference connected/supplied to the VersaSync, and once all other entries in the [Management](#) -> [Reference priority](#) table have been either disabled or deleted, the LED should no longer be blinking fast.

Temperature/temperature monitoring/High temperature alarms detected

A) Home page of the browser and *Tools* -> *System Monitor*

- Refer to the online VersaSync user guide at:
http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/OPRTN/StatMon_WebUI.htm

Temperature: The current **board temperature** will be displayed here.

» **Temperature(s):** Three temperatures are displayed:

- » **Oscillator temperature**, which has an effect on oscillator accuracy, and therefore can be used to interpret oscillator performance.
- » **Board temperature** (measured on the main board, sometimes also referred to as 'System temperature')
- » **CPU temperature**



B) “High Temp” Status LED/High Temperature alarms

- Refer to the online VersaSync user guide at:
http://manuals.spectracom.com/VSS/Content/VSS/INTRO/Fro_Pa_StatLEDs.htm

Management -> *Notifications* page of the browser, **System** tab

The screenshot shows the 'Notifications' configuration page for High Temperature alarms. It features four rows of settings, each with a checked checkbox, a radio button, a square icon, and a text input field. Below these are two sections for alarm thresholds: 'Minor Alarm Threshold' and 'Major Alarm Threshold'. Each section has two input fields: 'Minimum CPU Temperature (C)' and 'Readings above Threshold'.

The high temp indication (Major alarm) occurs at **100°C** (and a Minor temperature alarm occurs at **90°C**).

- (internal use only) The configuration file is located in `/etc/statusd/temperature.conf` however, it doesn't seem to be used by the WebUI. So it's not user-configurable.



	OFF	Temperature OK
	FAST	High temperature detected

Icon	Light	Meaning
	OFF	No network detected
	FAST	Network malfunction detected (e.g., no auto-negotiation)
	ON	Network OK, configuration OK
	OFF	Unit OK
	FAST	Unit requires attention; check other status LEDs, see Web UI
	HEARTBEAT	See table "LED Lighting Patterns" on page 4
	OFF	Temperature OK
	FAST	High temperature detected

Temperature-related FAQs

1 The VersaSync device has a "temperature alarm" status light. We would like to monitor this alarm remotely via REST. The web-GUI has three alarms (Oscillator, Board, and CPU). Which of the three corresponds to the physical alarm light on the box and what temperature level makes the LED start flashing?

A Keith's response (28 apr KW): The Temperature alarm status light is based on the **Board** (AKA "System") temp. The high temp indication (Major alarm) occurs at **100°C** (and a Minor temperature alarm occurs at **90°C**).

2 Regarding oscillator temperature, we believe we can monitor that temperature via REST, but what temperature is "bad". It's not clear from the documentation we have. Only a statement that temperature can effect oscillator performance.

A Keith's response: the oscillator in the VersaSync is designed to operate normally, through the entire VersaSync temperature range specification ("Temperature, in operation: -40°C to +71°C").

*Interfaces/connectors/cables (cabling)

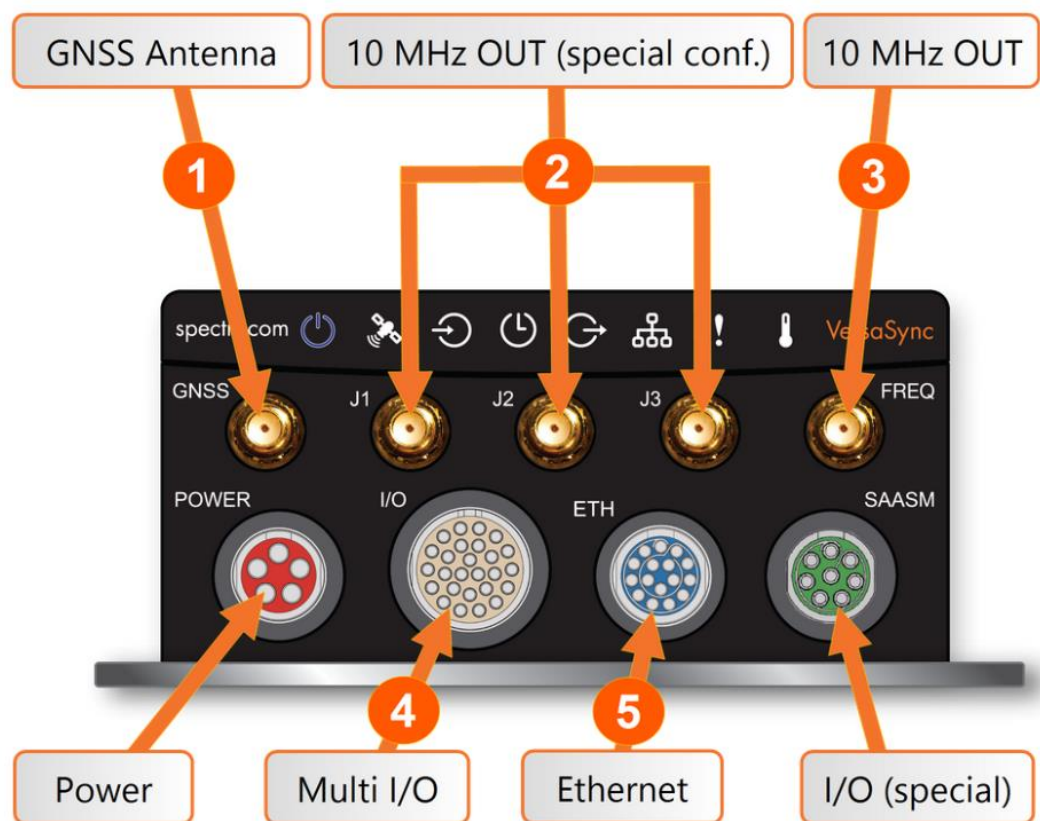
Email from Tom R: Florent did a document ("Interface Control Document") showing the VersaSync Interfaces. It is at https://app.bom.com/items/detail-spec?item_id=1221968409&version_id=10541866918&.

➤ This ICD document describes VersaSync interfaces:

- Electrical levels
- Connector pinouts
- Switching matrix

Info for all connectors/interfaces

➤ VersaSync user guide: http://manuals.spectracom.com/VSS/Content/VSS/INTRO/VSS_Interfaces.htm



Email from Tom Richardson to Dave L (12 Jul 16) All connectors are ODU AMC type. These connectors are circular mil type but not mil-spec.

ODU-USA Inc.
4010 Adolfo Road
Camarillo, CA 93012
United States of America
Phone: +1 (805) 484 0540
Fax: +1 (805) 484 7458
Email: sales@odu-usa.com

Note: Making the mating cable is not trivial and requires special tools. Customer should contact ODU for cable

assemblies. These parts are long lead and single source, anticipated 12 to 16 week deliveries.

Q For the Power and Ethernet connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

Q Hey guys, in trying to get the BNC cable from 17&18 to 11&12, the pin wings broke off. It would be better for the kit if you didn't populate the IO Cable Molex connector. The tooling to get those pins out is special, and I broke the tool trying to get the pins out ☺

What would be the cost to send me four new BNC cable pig tails with the pins on them.
Also, another empty IO Cable molex connector?

Essentially I need a BNC on 11&12, 13&14, 15&16, and 17&18.

A reply from Matt Loomis (30 June 2020 Here is the part details you are looking for to put together your cable.

I would suggest they use a 20 pin plug and add some connections. Parts are available from Mouser.
<https://www.mouser.com/Search/Refine?Keyword=043025-2000>

The mating plug part number to the VEK cable is **Molex 043025-2000**.



The pins are Molex part number 043030-0001 (reel) or 430300-0007(loose).



Hand crimp tool is Molex part number 63819-0000.



VersaSync Breakout cables

- The VersaSync's Breakout cables ARE NOT automatically included with every VersaSync.
- VersaSync Breakout cables are included in the optional (purchased separately) VersaSync Evaluation Kit (VEK)
 - Refer to "[VersaSync Evaluation kits \(VEK\)](#)" IN THIS DOCUMENT FOR MORE INFORMATION

Available protective dust caps kit (aka ODU AMC Soak caps)

- **1228-0000-0703:** VersaSync circular connector caps kit (non SAASM)
- Kit of dust caps for circular ODU connectors (power, LAN, I/O).
- No included in VEK
- **In Salesforce:** <https://orolia.lightning.force.com/lightning/r/Product2/01t1A000004sg4pQAA/view>
- **In Arena:** https://app.bom.com/items/detail-spec?item_id=1228289428&version_id=10653358328&orb_msg_single_search_p=1
- **In Online Versa user guide:** not currently included (as of May 2021)

Individual ODU AMC Mating Connector Plugs

- Info below is from the online VersaSync user guide at:
<http://manuals.spectracom.com/VSS/Content/VSS/SETUP/Connecting.htm>

The table below lists the part numbers for the mating connectors. The connectors can be ordered through Spectracom or ODU-USA Inc. All connectors are circular ODU AMC® "mil-type" connectors.

Connector Part Numbers

Ref	Description	VersaSync Connector		Mating (Cable) Connector	
		Spectracom Part No.	ODU Part No.	Spectracom Part No.	ODU Part No.
POWER	Power connector, 5 pin	J240R-0051-002Q	GK1YBR-P05UJ00-000L	P240R-0051-002Q	S11YBR-P05XJG0-0000
I/O	I/O connector, 26 pin	J240R-0261-002F	GK2YAR-P26UC00-000L	P240R-0261-002F	S12YAR-P26XCD0-0000
ETH	Ethernet connector, 16 pin	J240R-0161-002F	GK1YCR-P16UC00-000L	P240R-0161-002F	S11YCR-P16XCD0-0000
SAASM	Optional I/O connector, 8 pin	J240R-0081-012F	GK1YDR-P08UF00-000L	P240R-0081-002F	S11YDR-P08XFG0-0000

ODU® ordering contact information (USA):

- ODU-USA Inc.
4010 Adolfo Road
Camarillo, CA 93012
United States of America

Phone: +1 (805) 484 0540
Fax: +1 (805) 484 7458
Email: sales@odu-usa.com

Note: Building the mating cables requires special tools. Contact ODU for cable assemblies. Be advised that typical lead times are 12 to 16 weeks.

Available “VersaSync Mating Connectors Kits”

1. 1228-0000-0704: VersaSync Mating Connectors Kit, no SAASM

- Kit of **THREE** mating ODU AMC connectors for VersaSync (DC power, LAN, I/O) for customers to make custom cables with. **No pigtails.**
 - Not included in VEK ; connectors only - does not include wire. Allows customers to get quickly these long leadtime connectors, that they will provide to their specific cable suppliers
- **In Salesforce:** <https://orolia.lightning.force.com/lightning/r/Product2/01t1A000004sg4kQAA/view>
- **In Arena:** https://app.bom.com/items/detail-spec?item_id=1230188640&version_id=10689258028
- **In Online Versa user guide:** not currently included (as of May 2021)

Non-SAASM Kit consists of:

(1) **P240R-0051-002Q:** PLUG, ODU AMC SERIES,B KEY,5 PIN,M,SOLDER,22AWG,10A,450V



(1) **P240R-0161-002F** PLUG,ODU AMC SERIES,C KEY,16 PIN,M,SOLDER,26AWG,5A,300V



(1) **P240R-0261-002F** PLUG, ODU AMC SERIES, A KEY, 26 PIN, M, SOLDER, 26AWG, 5A, 300V



2. 1228-0000-0701: VersaSync Mating Connectors Kit, for SAASM

- Kit of **FOUR** mating ODU AMC connectors for VersaSync (DC power, LAN, I/O, SAASM) for customers to make custom cables with. **No pigtails.**
 - Not included in VEK ; connectors only - does not include wire. Allows customers to get quickly these long leadtime connectors, that they will provide to their specific cable suppliers
- **In Salesforce:** <https://orolia.lightning.force.com/lightning/r/Product2/01t1A000004xfAbQAI/view>
- **In Arena:** https://app.bom.com/items/detail-spec?item_id=1224822030&version_id=10689260108

SAASM Kit consists of:

- The same three ODU connectors above (in the no SAASM kit)

PLUS

- (1) **P240R-0081-002F** PLUG, ODU AMC SERIES,D KEY,8 PIN,M,SOLDER,22AWG,7A,333



Summary of the various Timing Input/Output signals (“Timing interfaces”)

Timing Signals

Timing Signal	Coding/Modulation	Input/Output	Connector
GNSS RF	L1 GPS, GLONASS 72 channels, T-RAIM integrity monitoring Option: L1/L2 SAASM	1 input	SMA, 5 VDC power supply to antenna
10 MHz	Sine, 10 dBm	1 outputs (standard) 4 outputs (optional)	SMA
Pulse/DCLS TTL level	1PPS, xPPS, IRIG, HaveQuick, alarm	Max: 2 inputs Max: 5 outputs	I/O connector
Pulse/DCLS 10 VDC	1PPS, xPPS, IRIG, HaveQuick, alarm	Max: 1 input Max: 1 output	I/O connector
RS232	NMEA 0183, other ASCII ToD formats	Max: 3 inputs Max: 3 outputs	I/O connector
RS485	HaveQuick, xPPS	Max: 3 inputs Max: 4 outputs	I/O connector
NTP over LAN (GbE)	NTP v3, v4; client, server	2	LAN connector
PTP over LAN (GbE)	PTP v1, v2; Master	2	LAN connector

A) Various Timing **INPUT** signals (Input Timing interfaces)

The following timing interfaces are provided:

Table 1-3: VersaSync inputs

INPUT SIGNAL	Total available	DCLS		RS-232	RS-485	ETH	Connector No. (see Fig. above)
		TTL	10V				
1PPS	(1)	1					4
ASCII/HaveQuick	(1)				1		4
ASCII/NMEA	(1)			1			4
Network Interface (10/100/1000bT): NTP (Stratum 2), PTP	(1)					1	5

B) Summary of various Timing **OUTPUT** signals (Output timing interfaces)

Table 1-4: VersaSync outputs

OUTPUT SIGNAL	Total available	DCLS		RS-232	RS-485	ETH	Connector No. (see Fig. above)
		TTL	10V				
10 MHz	(1+3)			SMA			2,3
1PPS	(2)	1	1				4
ASCII/HaveQuick	(1)				1		4
ASCII/NMEA	(1)			1			4
NTP server, PTP v2 master	(1)					1	5

Other Interfaces

- » USB serial equivalent: CLI interface (Connector 4)

Timing Outputs

DCLS Configurable (up to 3x TTL outputs, 1x 10V output)

- 1 PPS, any pulse up to 10 MHz
- IRIG B unmodulated, HaveQuick

RS232 and RS485 (up to 2 outputs)

- NMEA 0183 time of day message (GPZDA, GPRMC)
- HaveQuick

Frequency (x 1)

- 10 MHz, sine, +0 dBm, SMA connector

Network Interface (10/100/1000bT)

- NTP server (v3, v4)
- PTP IEEE1588 v1, v2 master

Front panel Connections

Front Panel Connections

Interface	Type of Data	Connector*
GNSS RF in	GNSS signal	SMA
Power in	DC power	Circular mil-type
Frequency out	10 MHz sine	SMA
Timing in/out	Pulse/DCLS, RS232, RS485; also USB communications	Circular mil-type
GbE	NTP, PTP Navigation messages Monitoring	Circular mil-type
SAASM keyloader	DS101, DS102	Circular mil-type

*connector pin-outs available in the user manual.

*Input Power connector/Standby Power (Input Power connector and Mil-STD standards for power)



Interface	Type of Data	Connector
Power in (1x)	DC power	Circular

- Input voltage (“*Vmain*”): 10-32vdc
- Input Power draw (“*Vmain*”): Typical 10W-12W
- Standby mode (“*Vstandby*”) (where only the oscillator is powered for faster startup): 0.4 W, DC power supply must be within 10.5-12VDC (has since been changed to within 10 to 32vdc, just like the “*Vmain*” input power).

Post-Boot Sequence, when Standby power is applied.

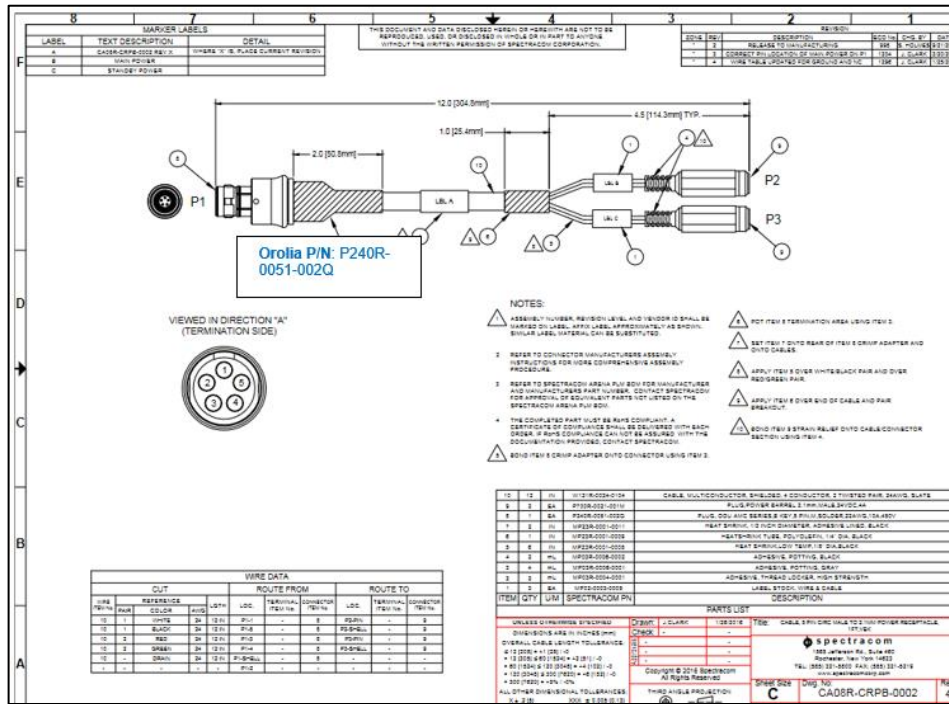
partial email from Ron Dries (~4 Apr 2019) *Vstandby* draws about 0.4 watts to keep oscillator, DAC, front panel CPLD running if it is connected but *Vmain* is not. **When in standby mode, I believe that the power indicator flashes at a slow rate.**

Confirmation from Mike Pratt with Engineering (17 Oct 2022) Hi Keith, we did confirm recently that the Versa Power LED will slowly pulse when the unit is on standby power only. I think this is not documented yet because standby power is not yet fully implemented as a feature.

The LED should not remain pulsing or blinking after booting up to main power.

Power cable (CA08R-CRPB-0002)

- Our P/N: CA08R-CRPB-0002 (in Arena at): https://app.bom.com/items/detail-spec?item_id=1225661540&version_id=10720108128



Individual Power Connector/Pinout info/FAQs

Associated Mating connector for power connector (as shown in cable drawing above)

Ref Des	Description	Spectracom part number	VersaSync Panel Connector (MFG and MFG P/N)	Spectracom P/N for Mating connector (to be used with external cable)	MFG and MFG P/N for Mating connector (to be used with external cable)
J14	Power connector, 5 pin	J240R-0051-002Q	ODU P/N: GK1YBR-P05UJ00-000L	P240R-0051-002Q	ODU P/N: S11YBR-P05XJG0-0000

DigiKey P/N for Power mating connector



- MFG (ODU) P/N S11YBR-P05XJG0-0000
- Digi-key P/N: 1907-1705-ND

➤ Refer especially to Salesforce Case 190477 where much of this info below was taken from

Q For the power and Ethernet connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

A) Pertaining to all three voltage pins (Vmain and Vstandby)

Q Do both “Vmain” and “Vbatt” (now labeled “Vstandby”) need to be connected to a power source?

A No

Q What happens when/if one of the terminals is not connected?

A (per Ron Dries ~4 Apr 2019) You do not need to connect both Vmain and Vstandby. Vmain operates the VersaSync.

If it is removed, VersaSync powers off. Vstandby input provided to keep oscillator running if Vmain is removed. If Vmain is not connected then VersaSync does not operate.

IF Vstandby is not connected, oscillator will power off when Vmain is removed.

IF Vmain is removed, but Vstandby is connected VersaSync will not operate, but oscillator, and disciplining hardware (DAC) is still on to keep oscillator running until Vmain is restored.

If both are connected, Vstandby current is negligible. Vstandby draws about 0.4 watts to keep oscillator, DAC, front panel CPLD running if it is connected but Vmain is not. When in standby mode I believe that the power indicator flashes at a slow rate.

B) Pins 1 and 2: (“Vmain..”) 10 to 32V

Q Do both Vmains and Vbatt need to be connected to a power source?

A No

Q What happens when/if one of the terminals is not connected?

A (per Ron Dries ~4 Apr 2019) You do not need to connect both Vmain and Vstandby. Vmain operates the VersaSync.

If it is removed VersaSync powers off. Vstandby input provided to keep oscillator running if Vmain is removed. If Vmain is not connected then VersaSync does not operate.

IF Vstandby is not connected, oscillator will power off when Vmain is removed.

IF Vmain is removed, but Vstandby is connected VersaSync will not operate, but oscillator, and disciplining hardware (DAC) is still on to keep oscillator running until Vmain is restored.

If both are connected, Vstandby current is negligible. Vstandby draws about 0.4 watts to keep oscillator, DAC, front panel CPLD running if it is connected but Vmain is not. When in standby mode I believe that the power indicator flashes at a slow rate.

C) Pin 3: “Vstandby” for available Standby power (J14) (was initially incorrectly labeled as “Vbatt”)

- VersaSync provides a low power mode that keeps the internal oscillator alive for restarting faster after a main supply outage.

Standby mode (only oscillator is powered): 0.4 W, DC power supply must be within 10.5-12VDC

Email from Mark McGregor (11 Jul 16): I would like to comment that the Vbat is 10.5V to 12V input voltage range. That may change in the future. I think it is supposed to be called standby power

partial email from Ron Dries (~4 Apr 2019) Vstandby draws about 0.4 watts to keep oscillator, DAC, front panel CPLD running if it is connected but Vmain is not. When in standby mode I believe that the power indicator flashes at a slow rate.

Q What is Vbatt?

A (per Ron Dries ~4 April 2019) The pin configuration on the VersaSync manual is incorrect, we are in the process of correcting it. The pinout should say Vstandby.

Q Does this imply that there is a battery inside the VersaSync?

A (per Ron Dries ~4 April 2019) The power cable does not imply that there is a battery inside VersaSync, but there is a battery inside VersaSync for RTC operation when power is removed. The customer has no electrical access to this battery. It is only connected to RTC chip

D) Ground pins

Q Are the Grounds to be used as Power Return? **Yes.**

A (per Ron Dries ~4 April 2019) Again please note that VersaSync is not compliant to MIL-STD-704. It does not comply with DC input power return is isolated from chassis.

Q Do the 2 grounds need to be isolated or can they be connected to the same GND/Return? **don't need to be isolated**

A (per Ron Dries ~4 April 2019) They can be connected together. They are connected together inside the VersaSync

Q Do the GNDs need to be isolated from Chassis GND? **No.**

A (per Ron Dries ~4 April 2019) The two cable GND are connected together and to chassis inside the VersaSync. Product internal GND and chassis GND are the same node electrically.

Certification of the breakout cables

Q Are the eval kit cables built by Orolia utilizing an aircraft certified classification so these can be used airborne (or are they round testing/reference only)?

A (per Ron Dries ~4 Apr 2019) The cables are not certified for aircraft. They are for lab integration.

DOD Military standards for input power (such as MIL-STD-1275 and Mil-STD-704)

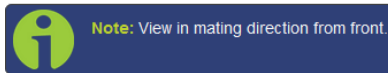
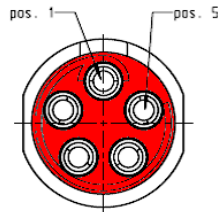
A) MIL-STD-1275 (CHARACTERISTICS OF 28 VOLT DC ELECTRICAL SYSTEMS IN MILITARY VEHICLES)

- Refer to sites such as: <https://militaryethernet.com/explaining-mil-std-1275/>

Q. Does VSync meet MIL-STD-1275 power spec?

A. reply from Tony D, 15 Mar 16 requires further investigation by our product management, as well as MIL-STD-704.

Pin-out



Note: View in mating direction from front.

Power connector pinout

Pin	Signal
1	V _{Main} (10 to 32 V)
2	V _{Main} (10 to 32 V)
3	V _{Batt} (10 to 32 V)
4	GND
5	GND

Q For the Power and Ethernet connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

B) MIL-STD-704: (MILITARY STANDARD: ELECTRIC POWER, AIRCRAFT, CHARACTERISTICS AND UTILIZATION OF)

- Refer to sites such as: <https://en.wikipedia.org/wiki/MIL-STD-704>

MIL-STD-704 Aircraft Electrical Power Characteristics is a [United States Military Standard](#) that defines a standardized power interface between a [military aircraft](#) and its equipment and carriage stores, covering such topics as voltage, frequency, phase, power factor, [ripple](#), maximum current, [electrical noise](#) and abnormal conditions (overvoltage and undervoltage), for both AC and DC systems.

- As of at March 2020 (per Dave Sohn) the VersaSync (and VersaPNT) does not meet MIL-STD-704 requirements.

Email from Dave Sohn (18 March 2020) "Versa does not meet MIL-STD-704 requirements."

- Note See email further below from Ron Dries as to why.

Q (referring to the Lithium battery for the RTC) can you provide specification for purposes of flightworthiness analysis?

A (per Ron Dries 4 Apr 2019) The RTC battery is a Seiko MS920T-FL27E. It is a low capacity rechargeable lithium. I do not know what a spec for purposes of flight worthiness is, however, please note that VersaSync can't be used for any flight or safety critical application **because it does not meet MIL-STD-704 requirement of operation for 7 seconds with 0V DC input voltage.**

Status update – email from Chris Shannon (28 July KW) Well.... It doesn't have to work without power. It can reboot without permanent damage and pass that test. I'm looking at a SATCOM modem MIL-STD-704 LDC601 test that passed.....check this out (from an actual 704 test report):

TABLE LDC601-III. Data sheet for LDC601 power failure.

Test Condition	Parameters				Performance
	Voltage		Time Duration of Power Failure		
A	28	V _{DC}	100	msec	Pass
B	28	V _{DC}	500	msec	Pass
C	28	V _{DC}	3	sec	Pass
D	28	V _{DC}	7	sec	Pass

Summary:

During each occurrence of the events above, the EUT would reboot. No permanent damage was caused and the EUT returned to normal operation every time.

I added in my reply "I cant comment on other customers of the VersaSync, and potential flight hours. But Charles or Tony DiFlorio may be able to:

Reply from Tony Diflorio (29 July 2020) to the customer: We have customers who have flown the VersaSync. I have personally worked with SNC (Sierra Nevada Corp) as the prime contractor on a project for the Army at APG. The program name is not public but they use "Project C" for the identifier. They have VersaSync units in aircrafts. The integrator is ViaSat.

**Ethernet Interface (Ethernet) connector

- VersaSync provides two different Gigabit Ethernet links (Eth0 and Eth1)



Interface	Type of Data	Connector
Ethernet in/out	NTP, PTP Navigation messages Monitoring	Circular

Mating connector

P240R-0161-002F: In Arena at: https://app.bom.com/items/detail-spec?item_id=1214648083&version_id=10607724398

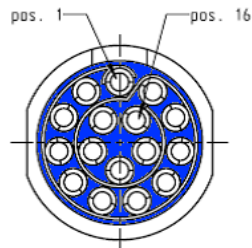
Ref Des	Description	Spectracom Part Number	VersaSync Panel Connector	Mating connector (to be used for external cable)	Spectracom mating part number
J2	Ethernet connector, 16 pin	J240R-0161-002F	GK1YCR-P16UC00-000L	S11YCR-P16XCD0-0000	P240R-0161-002F

Pin-out

J2, Ethernet

- 1 through 8 – A Ethernet Connect, 4 pairs, 1000bT
- 9 through 16 – B Ethernet Connect, 4 pairs, 1000bT

Ethernet Connector



Note: View in mating direction from front.

The Ethernet connector provides two 1GbE network connections, using 8 wires (pinout below).

Ethernet connector pinout

Pin	Signal	Pin	Signal
1	Ethernet_1 A+	9	Ethernet_2 A+
2	Ethernet_1 A-	10	Ethernet_2 A-
3	Ethernet_1 B+	11	Ethernet_2 B+
4	Ethernet_1 B- ETH0	12	Ethernet_2 B- ETH1
5	Ethernet_1 C+	13	Ethernet_2 C+
6	Ethernet_1 C-	14	Ethernet_2 C-
7	Ethernet_1 D+	15	Ethernet_2 D+
8	Ethernet_1 D-	16	Ethernet_2 D-

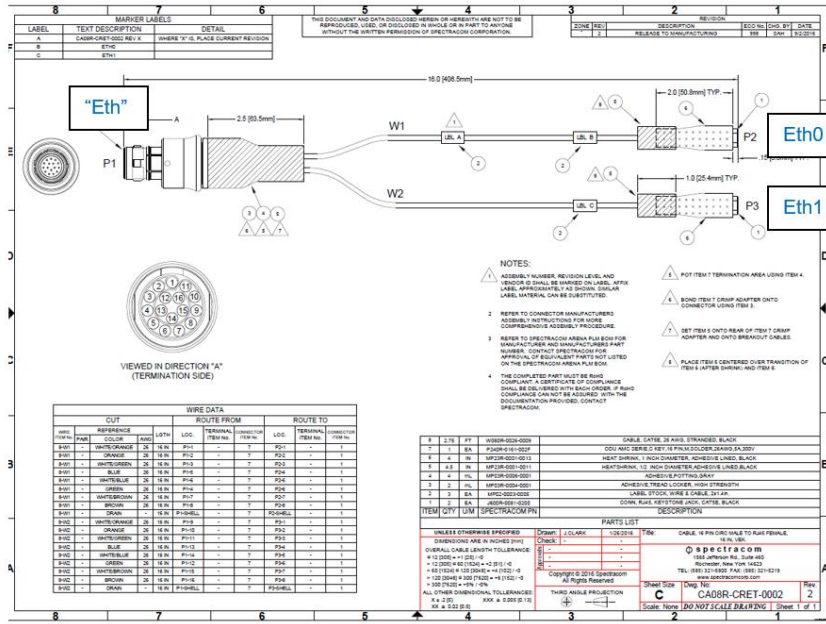
It is also possible to wire your connector to 100MbE, using only 4 wires. Contact Tech Support for more information.

The pinouts described above are from the hardware design. They correspond with the software naming convention of interfaces as follows: Ethernet_1 is referred to as "eth0" in the system and Web UI, and Ethernet_2 is referred to as "eth1".

**Ethernet breakout cable (CA08R-CRET-0002) for eth0 and eth1

Note: Breakout cables are not included with the purchase of base VersaSync. They are included with purchase of optional VersaSync Evaluation Kit (VEK).

- Our P/N: **CA08R-CRET-0002** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1225621958&version_id=11339902938&orb_msg_single_search_p=1)



Certification of the breakout cables

Q Are the cables built by Orolia utilizing an aircraft certified classification so these can be used airborne (or are they round testing/reference only)?

A (per Ron Dries ~4 Apr 2019) The cables are not certified for aircraft. They are for lab integration.

Q For the Power and Ethernet ODU connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

four wire 100 MB ethernet connection only (not for use with 1GB connections)

Ethernet connector pinout

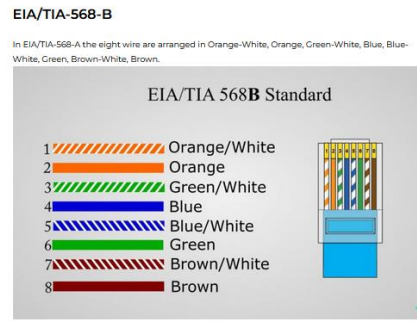
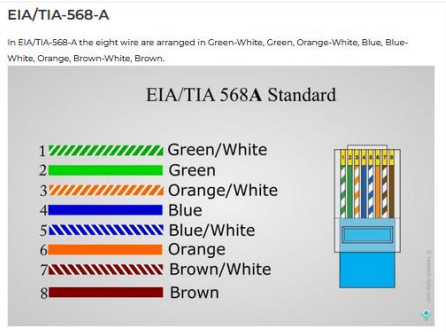
Pin	Signal	Pin	Signal
1	Ethernet_1 A+	9	Ethernet_2 A+
2	Ethernet_1 A-	10	Ethernet_2 A-
3	Ethernet_1 B+	11	Ethernet_2 B+
4	Ethernet_1 B-	12	Ethernet_2 B-
5	Ethernet_1 C+	13	Ethernet_2 C+
6	Ethernet_1 C-	14	Ethernet_2 C-
7	Ethernet_1 D+	15	Ethernet_2 D+
8	Ethernet_1 D-	16	Ethernet_2 D-

It is also possible to wire your connector to 100MbE, using only 4 wires. Contact Tech Support for more information.

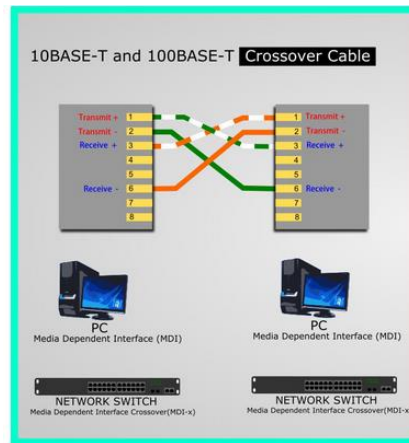
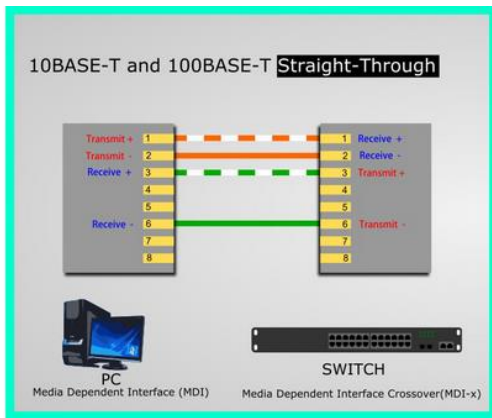
- Refer to Salesforce Case 238463

A) Background details

- Ethernet cables have available **8 wires (four pairs of green, orange, blue, brown)**

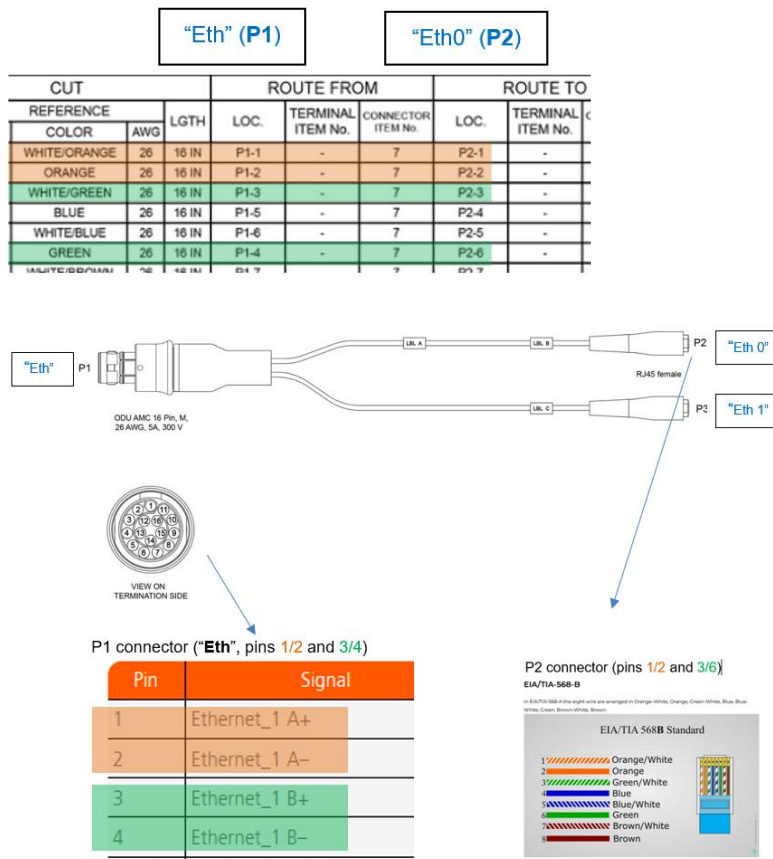


- **100MB** only needs total of **4 wires** (only **two pairs- the green and orange**= of the available four pairs)



- **1000MB (1GB)** requires all **8 wires** be used (all **four pairs** are used)

B) Four Wire Pinout Details



The four wire ethernet should be using the P1 pins 1, 2, 3 and 4. These correspond with 1, 2, 3 and 6 of the RJ45 connector using the **Orange** and **Green** pairs. That is all that is required. The RJ45 is shown as P2 on this diagram of the Ethernet data cable wiring.

Q The manual mentions a four wire 100 MB ethernet connection, but I cannot find any information on how to do this. What wire connections are necessary and are any specific configurations required?

A Reply from Dave L (2 July 2020) We discussed this in our engineering meeting this morning. From what I was told, the VersaSync ethernet port is auto-sensing the port speed and duplex so this should not be problem. I was also told the pin connections you have are correct.

If you have the four wire ethernet cable going from the laptop to the VersaSync pigtail cable you may need a crossover cable to make it work. Going from the switch to the VersaSync should not require a crossover cable.

The VersaSync has two ethernet ports. Please make sure you are using the ethernet 0 setup.

Otherwise, please check the continuity of the pigtail cable pins **P1 1-4** to **P2 1-3 and 6**. The cable may be faulty. Let me know if you have any success using the C and D connections for eth 1.

****Multi “I/O” connector** (Inputs/Outputs, such as USB/Serial for CLI interface, 1PPS, ASCII, IRIG, etc)



Interfaces (Power, Communications, I/O)

Interface	Type of Data	Connector
GNSS RF in (1x)	GNSS signal	SMA
Power in (1x)	DC power	Circular
Frequency out (1x)	10 MHz sine	SMA
GPIO in/out	Up to 3x TTL and 1x 10V outputs Any rate up to 10MHz IRIG B (unmodulated) HaveQuick	Circular
RS232 in/out	Up to 2x RS232 outputs NMEA messages Binary navigation data	Circular
RS485 in/out	Up to 3x RS485 outputs NMEA messages Binary navigation data	Circular
Ethernet in/out	NTP, PTP Navigation messages Monitoring	Circular
USB	1 USB connector	Circular
SAASM keyloader	DS101, DS102	Dedicated circular connector

Q For the Power and Ethernet ODU connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

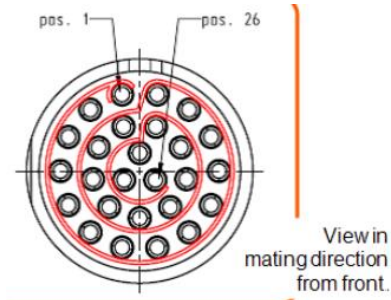
Mating connector

P240R-0261-002F: in Arena at: https://app.bom.com/items/detail-spec?item_id=1214648064&version_id=10607724158

Ref Des	Description	Spectracom part number	VersaSync Panel Connector	Mating connector (to be used for external cable)	Spectracom mating part number
J1	I/O connector, 26 pin	J240R-0261-002F	GK2YAR-P26UC00-000L	S12YAR-26XCD0-0000	P240R-0261-002F

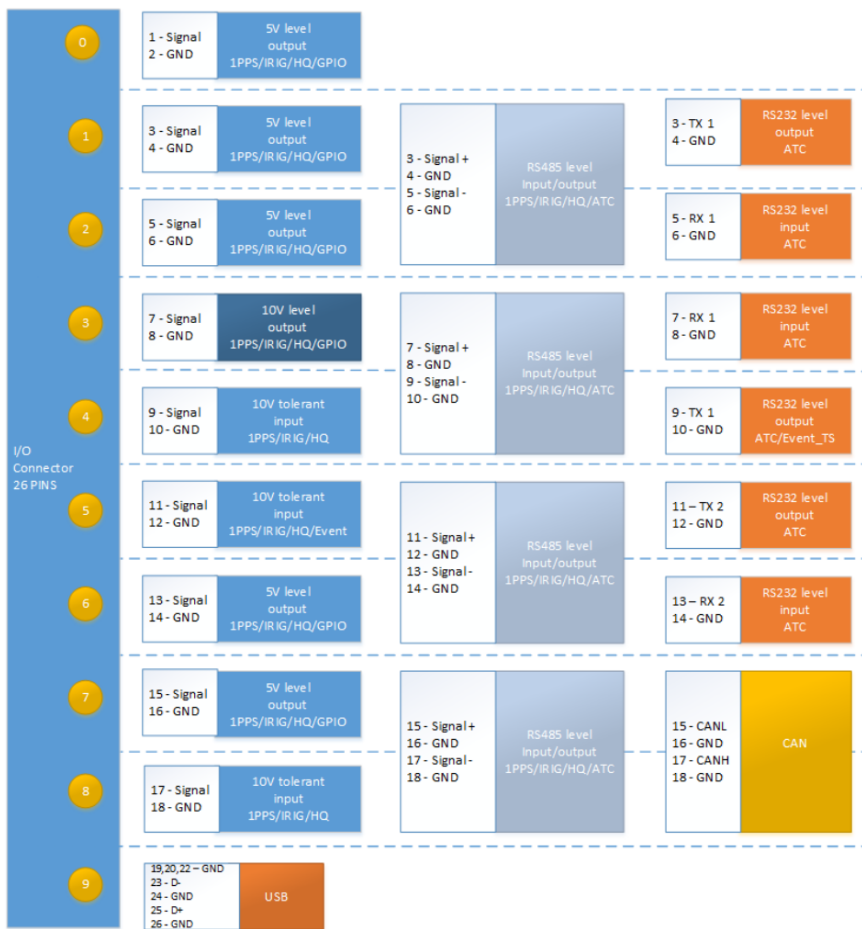
Assigning I/O pins

- Refer to online VersaSync user guide: <http://manuals.spectracom.com/VSS/Content/VSS/SETUP/IOPinConfiguration.htm>
- the I/O connector is software configurable, i.e. the pin interfaces and the signal modulations can be configured by the user via the VersaSync Web UI.
- The software-configurable 26-pin I/O connector comprises 9 user-configurable Channels, plus one fixed USB interface. Channels can be used for the following input or output interfaces:



Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (5V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal -)	19	9 (USB dedicated)	GND
6		GND	20		GND
7	3	1PPS output (10 V)	21		Not connected
8		GND	22		GND
9	4	ASCII output (RS-232)	23		USB D-
10		GND	24		GND
11	5	1PPS input	25		USB D+
12		GND	26		GND
13	6	ASCII input (RS-232)			
14		GND			



Signal Types

The table below shows the maximum number of available interfaces for each signal type. Note that you can assign only one signal for each pin pair, hence only four to nine input and output signals can be transmitted/received at any given time. For details see the interactive Configurator below.

Available signal types

	DCLS, TTL	DCLS, 10V	RS485	RS 485, 120 Ω	RS232
PPS	out (5), in (2)	out (1), in (1)	out (4), in (4)	in (4)	
IRIG	out (5), in (2)	out (1), in (1)	out (4), in (4)	in (4)	
HQ	out (5), in (2)	out (1), in (1)	out (4), in (4)	in (4)	
GPIO	out (5)	out (1)			
ASCII			out (4), in (4)	in (4)	out (3), in (3)

Note: ASCII Time Code is abbreviated in the UI as **ATC**.

DCLS Signal Lines

- Up to six TTL (5V) or 10 V DCLS outputs and three DCLS inputs are available for e.g., 1PPS, xPPS, IRIG B 00x, HaveQuick, ASCII ToD signal transmission.

Single-ended Serial Lines

- VersaSync provides up to 3 RX and 3 TX RS232 interfaces for e.g., ASCII ToD – NMEA 0183 (ICD-GPS-153).

Differential Serial Lines

- Up to four differential serial lines are available. Each of them can be set in either RS422 or RS485 electrical standard, and used as input or output. One can be used in CAN mode. PPS or Time-of-Day messages will be available, as well as HaveQuick and ICD GPS-060. Note that this kind of interface uses two Channels.

Non-Configurable Pins

- Channel # 0 provides a DCLS TTL output signal that is not user-configurable.
- Also note that pins # 19 through 26 are reserved for the USB command line interface.

I/O Signal Mapping Table

Each Channel (i.e., each pin pair e.g., "3&4" = Channel 1) can serve as only one interface, and not all combinations are possible due to the internal multiplexer architecture.

The table below illustrates the signal combinations that can be assigned to the 18 configurable pins.

I/O signal mapping to Channels

				Channel									
				0	1	2	3	4	5	6	7	8	9
				Pin Position									
				1 & 2	3 & 4	5 & 6	7 & 8	9 & 10	11 & 12	13 & 14	15 & 16	17 & 18	19-25
Time & Frequency	Signal Message Type	I/O	Type Filter	Electr. Level									
	PPS	out	DCLS	TTL	Y	Y	Y				Y	Y	
	IRIG	out	DCLS	TTL	Y	Y	Y				Y	Y	
	HQ	out	DCLS	TTL	Y	Y	Y				Y	Y	
	GPIO	out	DCLS	TTL	Y	Y	Y				Y	Y	
	ATC	out	RS232						Y	Y			
	PPS	out	RS485			Y		Y		Y		Y	
	IRIG	out	RS485			Y		Y		Y		Y	
	HQ	out	RS485			Y		Y		Y		Y	
	ATC	out	RS485			Y		Y		Y		Y	
	PPS	in	RS485			Y		Y		Y		Y	
	PPS	in	RS485	Load		Y		Y		Y		Y	
	IRIG	in	RS485			Y		Y		Y		Y	
	IRIG	in	RS485	Load		Y		Y		Y		Y	
	HQ	in	RS485			Y		Y		Y		Y	
	HQ	in	RS485	Load		Y		Y		Y		Y	
	ATC	in	RS485			Y		Y		Y		Y	
	ATC	in	RS485	Load		Y		Y		Y		Y	
	ATC	in	RS232				Y				Y		
	PPS	out	DCLS	10V				Y					
	IRIG	out	DCLS	10V				Y					
	HQ	out	DCLS	10V				Y					
	GPIO	out	DCLS	10V				Y					
	PPS	in	DCLS	10V					Y				
	IRIG	in	DCLS	10V					Y				
	HQ	in	DCLS	10V					Y				
	PPS	in	DCLS	TTL						Y			Y
	IRIG	in	DCLS	TTL						Y			Y
	HQ	in	DCLS	TTL						Y			Y
	OPTION CARD												
CAN BUS	in/out				Y	Y	Y	Y	Y	Y	Y	Y	

Occupied - USB

Notes:

Pins to Channels (e.g., pins 3 & 4= Channel 1)

green = Signal Message Type can be assigned to this Channel (RS485 requires two Channels)

red = This Signal Message type cannot be assigned to this Channel

ATC = ASCII Time Code

Interactive I/O Configurator

Each Channel can serve as only one interface, and not all combinations are possible due to the internal multiplexer architecture. Use the interactive I/O switch matrix below to design your I/O configuration by dragging any signal type from the left-hand column to one of the highlighted fields.

Versasync Configuration Tool						
	DCL5	RS485	RS232	Open	Pins	SETUP
Selector	OUT TTL				1-2	
PPS	OUT TTL		TX		3-4	
IRIG	OUT TTL		RX		5-6	
ASCS	OUT TTL					
HQ	OUT 10V		RX		7-8	
CAN	IN 10V		TX		9-10	
GPIO	IN TTL		TX		11-12	
EVENT	OUT TTL		RX		13-14	
(Drag Here to Assign)	OUT TTL				15-16	
Reset	IN TTL		CAN		17-18	

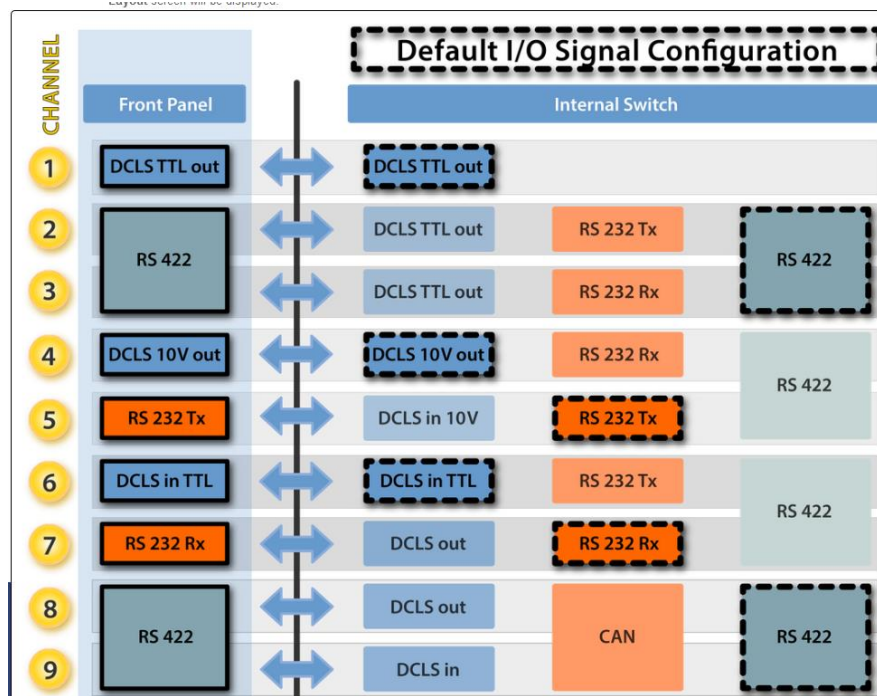
Configuring a new Input or Output

1. In the VersaSync Web UI, navigate to **MANAGEMENT** > **NETWORK: Pin Layout**. The Pin Layout screen will be displayed.
2. Prior to assigning the new output, identify a pin pair in the pin Layout table that is not used (Signal = "None") or not needed. You can Delete it, but you may also simply assign the new PPS Output as described below, thus overwriting the existing Input or Output.
3. Add a pin configuration by clicking the PLUS icon in the top-right corner. The Add Pin window will display.
4. Start with the Type Filter drop-down menu (second line in the window) and select a signal type.
5. From the Signal drop-down menu, select a signal.
6. From the Pins drop-down menu in line 3, select the pin pair you chose in Step 2. (Note that you will need 4 pins if you selected a RS485 signal Type.)
7. Click Submit.
8. In the Actions panel, click **Apply Changes**.

Default I/O Signal Configuration pinout

Restoring the Default I/O Configuration

- VersaSync is shipped with a default I/O configuration that you can be customized. However, if required you can restore the default configuration at any time after applying changes.
- The following illustration shows the default I/O pin configuration:



To restore the default I/O pin configuration:

1. Navigate to the **MANAGEMENT: NETWORK > Pin Layout** screen.
2. In the Actions panel on the left, click Restore Default Layout.

Multi I/O Cable (USB Connector for terminal connection) and I/O breakout cable



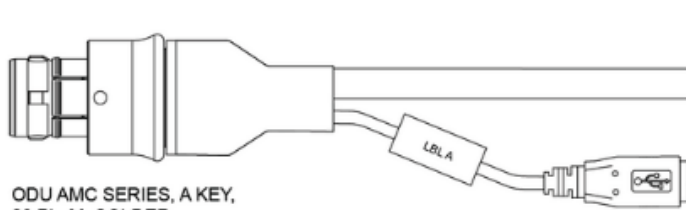
Interfaces (Power, Communications, I/O)

Interface	Type of Data	Connector
GNSS RF in (1x)	GNSS signal	SMA
Power in (1x)	DC power	Circular
Frequency out (1x)	10 MHz sine	SMA
GPIO in/out	Up to 3x TTL and 1x 10V outputs Any rate up to 10 MHz (RIG 8 (unmodulated) HaveQuick)	Circular
RS232 in/out	Up to 2x RS232 outputs NMEA messages Binary navigation data	Circular
RS485 in/out	Up to 3x RS485 outputs NMEA messages Binary navigation data	Circular
Ethernet in/out	NTP, PTP Navigation messages Monitoring	Circular
USB	1 USB connector	Circular
SAASM keyloader	DS101, DS102	Dedicated circular connector

A) I/O cable (CA08R-CRUB-0002)

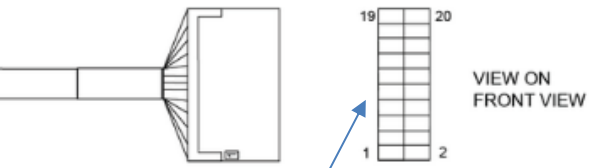
Note: Breakout cables are not included with the purchase of base VersaSync. They are included with purchase of optional VersaSync Evaluation Kit (VEK).

- The I/O cable attaches directly to the Versa
- The I/O breakout cable connects to the end of the I/O cable
- **Our P/N for I/O cable: CA08R-CRUB-0002** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1225629893&version_id=11356104258)



ODU AMC SERIES, A KEY,
26 Pin M, SOLDER
26 AWG, 5A, 300 V

CABLE USB TYPE A



VIEW ON FRONT VIEW



VIEW ON TERMINATION SIDE

USB connector for terminal connection (USB to Serial)

Note: The pin diagrams show the "solder/wiring" (under the cover) side of the connector.

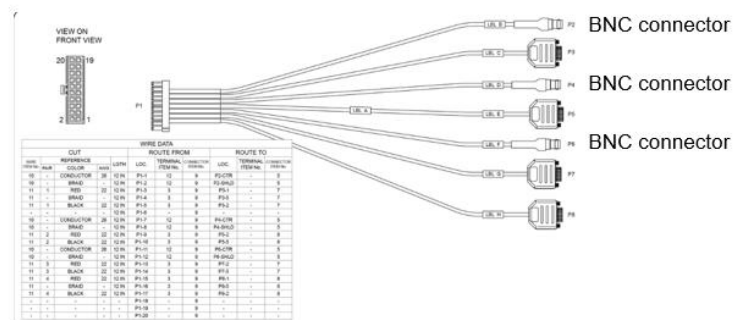
The "interface" side of the connector has the same pin numbers as shown, but the pin locations will be opposite of the pin locations shown.

CUT		To I/O breakout cable (shown further below)		ROUTE TO	
WIRE TERMINAL	PAIR	REFERENCE COLOR	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.
11	1	BLACK/RED	26 12 IN P1-1	P2-1	10 9
11	1	RED/BLACK	26 12 IN P1-2	P2-2	10 9
11	2	BLACK/WHITE	26 12 IN P1-3	P2-3	10 9
11	2	WHITE/BLACK	26 12 IN P1-4	P2-4	10 9
11	3	BLACK/GREEN	26 12 IN P1-5	P2-5	10 9
11	3	GREEN/BLACK	26 12 IN P1-6	P2-6	10 9
11	4	BLACK/BLUE	26 12 IN P1-7	P2-7	10 9
11	4	BLUE/BLACK	26 12 IN P1-8	P2-8	10 9
11	5	BLACK/YELLOW	26 12 IN P1-9	P2-9	10 9
11	5	YELLOW/BLACK	26 12 IN P1-10	P2-10	10 9
11	6	BROWN/BLACK	26 12 IN P1-11	P2-11	10 9
11	6	BLACK/BROWN	26 12 IN P1-12	P2-12	10 9
11	7	BLACK/ORANGE	26 12 IN P1-13	P2-13	10 9
11	7	ORANGE/BLACK	26 12 IN P1-14	P2-14	10 9
11	8	RED/WHITE	26 12 IN P1-15	P2-15	10 9
11	8	WHITE/RED	26 12 IN P1-16	P2-16	10 9
11	9	RED/GREEN	26 12 IN P1-17	P2-17	10 9
11	9	GREEN/RED	26 12 IN P1-18	P2-18	10 9
11	10	RED/BLUE	26 12 IN P1-19	P2-19	10 9
11	10	BLUE/RED	26 12 IN P1-20	P2-20	10 9
1	-	RED	- - P1-21	P3-1	- 1
-	-	-	- - P1-22	-	- -
1	-	WHITE	26 3.5 IN P1-23	P3-2	- 1
1	-	BLACK	26 3.5 IN P1-24	P3-4	- 1
1	-	GREEN	26 3.5 IN P1-25	P3-3	- 1
-	-	-	- - P1-26	-	- -
11	-	SHIELD	- 12 IN P1-SHELL	-	- -
1	-	DRAIN	- 3.5 IN P1-SHELL	P3-SHELL	- 1

B) I/O Breakout cable (CA08R-3M00-0001)

Breakout cables are not included with the purchase of base VersaSync. They are included with purchase of optional VersaSync Evaluation Kit (VEK).

- Refer to online VersaSync user guide: <http://manuals.spectracom.com/VSS/Content/VSS/SETUP/ToolsCables.htm?Highlight=breakout>
- Our P/N for I/O breakout cable: **CA08R-3M00-0001** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1225739985&version_id=10643174068&orb_msg_single_search_p=1)



Per Ron Dries (5 Aug 2020) the I/O breakout cable in the EVK only has RS-232 (DB9) and BNC connectors on it
Certification of the breakout cables

Q Are the cables built by Orolia utilizing an aircraft certified classification so these can be used airborne (or are they round testing/reference only)?

A (per Ron Dries ~4 Apr 2019) The cables are not certified for aircraft. They are for lab integration.

INPUTS

*****IRIG inputs/outputs

- Uses the Multi I/O connector on the VersaSync/PNT



Timing Signals

Timing Signal	Coding/Modulation	Input/Output	Connector
Pulse/DCLS TTL level	1PPS, xPPS, IRIG, HaveQuick, alarm	Max: 2 inputs Max: 5 outputs	I/O connector
Pulse/DCLS 10 VDC	1PPS, xPPS, IRIG, HaveQuick, alarm	Max: 1 input Max: 1 output	I/O connector

A) IRIG DCLS inputs/outputs

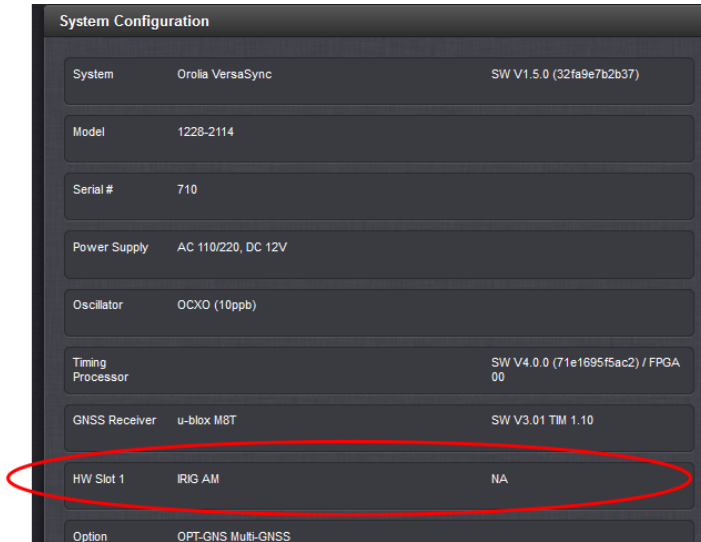
- available (in all models/all software versions) via I/O connector

B) IRIG AM (1) IRIG AM Input and (3) IRIG AM outputs via Option Card (VersaSync Models 1228-2xx4)

Links/shortcuts for IRIG AM

- In Salesforce:
- **Schematic for IRIG Option Card (P/N: 1228-1001-0230)** in Arena: https://app.bom.com/items/detail-spec?item_id=1252352621&version_id=11174316558&
- Test procedure for Option Card (1228-2114-3000-TP)
- Refer to online SecureSync user guide: http://manuals.spectracom.com/VSS/Content/VSS/APP/IRIG_AM_OC.htm

IRIG AM input/output is added via an installed Option Card.



- refer to **ECO-FAI-001906** (Jan 2019) for the release of the IRIG option board to Production (in Arena): https://app.bom.com/changes/detail-affected?change_id=2395284510
 - this page in Arena Contains parts list, schematic, etc for the IRIG option board

Software version-related info for IRIG AM Option

- IRIG AM output capability first added in software version **1.3.1C**.
- More recent versions 1.3.k 1.4.0, 1.4.1, 1.4.2 etc are NOT compatible with IRIG AM (the browser configuration for IRIG will be lost if the VersaSync is updated)
- **Version 1.5.0** merged the 1.3.1c IRIG AM function into the main VersaSync trunk.
 - Until version 1.5.0 was released (Q4 2021), **Version 1.3.1C ONLY** is compatible with IRIG AM

Software Update stops at “Executing Transfer Scripts”

- Due to trying to update v1.3.1c to a more recent version which doesn't support IRIG AM (such as to versions 1.3.1k, 1.4.0, 1.4.1, etc)



(June 2020) We've had a firmware upgrade failure on another versasync unit. We were in the process of upgrading from 1.3.1c to 1.3.1k and it stops at "ExecutingTransfer Scripts" (firmware_upgrade1.png attached). We were also monitoring the serial output (firmware_upgrade2.png) and we can see that it went through the reboot process but upon boot, it looks like the boot is corrupted somehow. At this point, if we attempt to boot it, we simply get the "File not found boot/soc_system.rbf" message and the fpga usage message.

None of the lights on the unit come up. Prior to performing the upgrade, we did confirm that there is plenty of free space (15% utilization). Is there anything we can do at this point

Customer desire to add IRIG AM Option to a fielded unit (previously purchased, without IRIG option card being installed at time of purchase)

- Refer to Case 204691

Limitations/Requirements to add IRIG AM option to a fielded unit

1. **Minimum software version: 1.3.1C only** (no other version besides 1.3.1c until at least version 1.5.0 has been released in 2021)
2. **Can't have SAASM receiver installed (??)** Space for only one Option card in a Versa. SAASM and IRIG are both Options via an installed Option Card. So not enough room to install both simultaneously??? (need to confirm)

Email from Keith to Tony D, Jon S and Dave S (2 Aug 19) in reference to case 204691, regarding Greg Johnston with US Army wanting to add IRIG AM option to an already fielded VersaSync, I was assigned this case (Salesforce Case Number 204691).

I haven't run across this particular scenario before. I'm not sure if we are authorizing customers to be able to purchase just a VersaSync/PNT Option Card, such as IRIG AM, and to install it themselves locally (as we do with SecureSyncs). If this is the case, the Services/RMA Teams don't even need to be involved. Customers can simply purchase the Option card thru Sales.

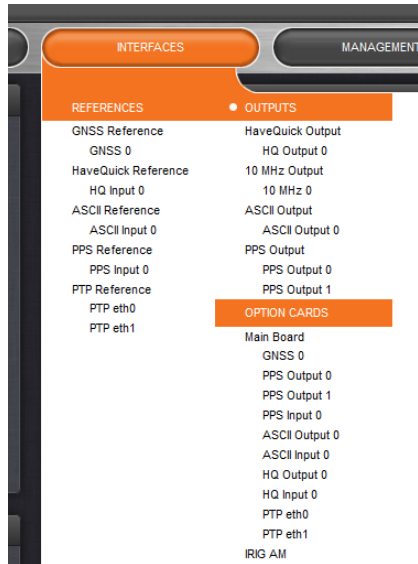
If VersaSync Option Cards are not intended to be installed locally by customers, I assume they just need to purchase the IRIG AM Option thru Sales (at the option purchase cost, plus a markup for the rework?? In the past, we typically charged 1 ½ times the Option price to add an option after the original sale). Then, an RMA Number can be assigned for the mod.

Other than a minimum software version being installed (version 1.3.1c) I'm not aware of any other potential limitations on purchasing/installing this option card for a fielded VersaSync.

Hi Jon (and Dave S),
Please let me know your thoughts for a customer desiring to add IRIG AM input to an existing VersaSync. For our future reference, are there any other limitations to adding IRIG AM card, besides the minimum software version of 1.3.1C which I understand added support for IRIG AM output?

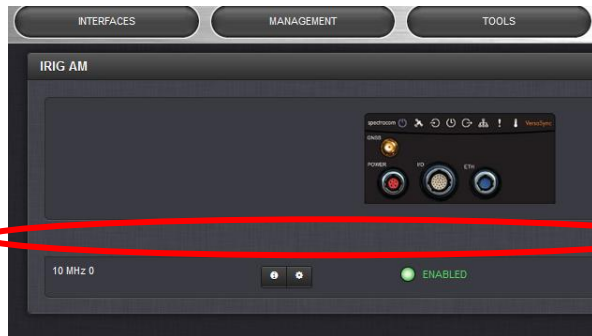
IRIG AM input/output configuration

Interfaces -> **IRIG AM** (under Option Cards)



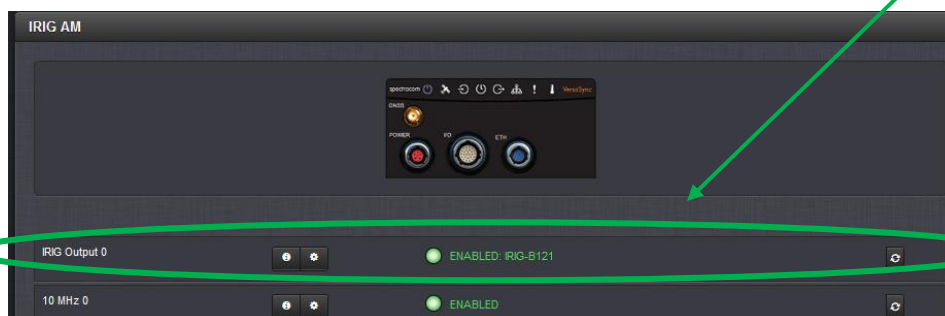
Note Have to configure Pin Configuration with IRIG signals, before being able to edit the IRIG AM Settings

A) Before enabling IRIG AM in *Pin Layout* page of the browser



No IRIG AM configuration available until IRIG AM pins are configured in the *Management* -> *Pin Layout* page of the browser

B) After enabling IRIG AM in *Pin Layout* page of the browser



IRIG Output 0

IRIG-B121

Signature Control: Output Always Enabled

Format: (B) IRIG B

Modulation: (1) IRIG AM Only

Frequency: (2) 1 KHz

Amplitude: 128

Coded Expression: (1) BCD TOY, CF

Control Function Conformance: RCC 200-04

Timescale: UTC

Offset: 0

Status Submit

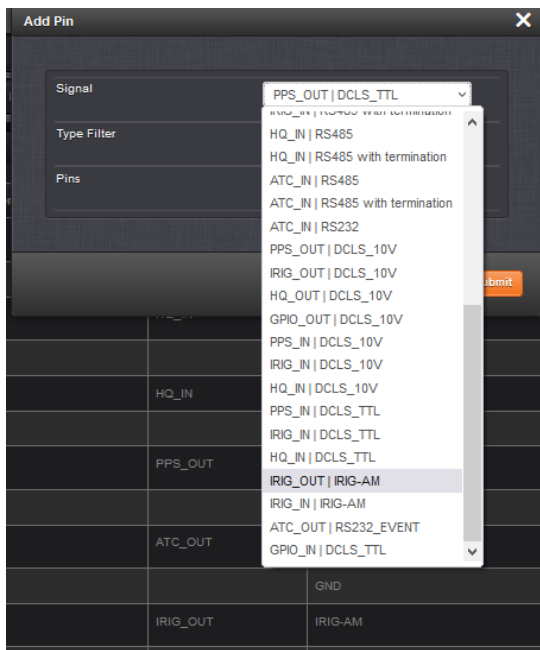
I/O PIN Layout configuration with IRIG AM Option Card installed

Email from Dave Lorah about still having GPIO pins available when IRIG AM pins are configured (Nov 2021) I am now able to confirm the VersaSync, with v1.5.0 firmware and the IRIG Option card installed, will output GPIO functions on the **pins 11, 12 (Input) and 13, 14, 15, 16 (Outputs)**

Pins 17 and 18 provide PPS, IRIG and HQ Inputs only.

Management -> **Pin Layout** page of the browser

- 1) Press the "+" on right side to edit the layout table
- 2) Change Signal" to either "IRIG_Out or "IRIG_In"



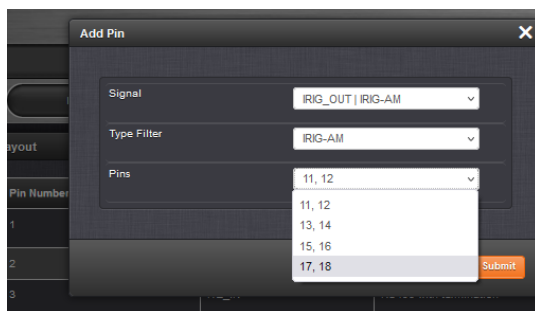
3) Change “Type Filter:” to “**IRIG AM**”

4) Select the desired pins for the IRIG AM signal

Note: (IRIG AM input and/or output Pins are limited to just pins 11 and 12, pins 13 and 14, pins 15 and 16 or 16, 18

Email from Dave Lorah about still having GPIO pins available when IRIG AM pins are configured (Nov 2021) I am now able to confirm the VersaSync, with v1.5.0 firmware and the IRIG Option card installed, will output GPIO functions on the **pins 11, 12 (Input) and 13, 14, 15, 16 (Outputs)**

Pins 17 and 18 provide PPS, IRIG and HQ Inputs only.



5) On the left, press “**Apply Changes**”

Note: “**Save Layout**” allows just the pin configuration to be exported as a file. It’s not necessary to “save layout” after a change to the pin layout.

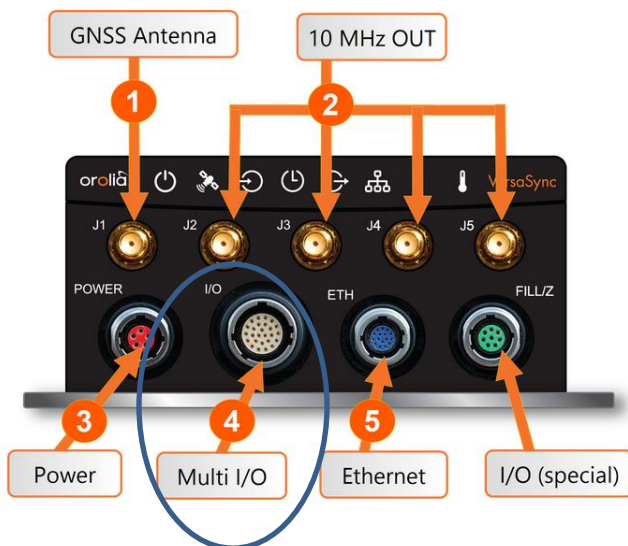
IRIG Formats

- Online user guide (July 2021) states: **Format: [(A) IRIG A, (B) IRIG B, (G) IRIG G, (N) NASA 36, (E) IRIG E]** (no IRIG H mentioned)

(July 2021) Is IRIG H supported in VersaSyncs?

- (July 2021) Customer purchased and said not available in unit (refer to Salesforce Cases 265028/269642)
- Online user guide (July 2021) states: **Format: [(A) IRIG A, (B) IRIG B, (G) IRIG G, (N) NASA 36, (E) IRIG E]** (no IRIG H mentioned)
- Online Versa User guide makes it look like IRIG H is available (listed in table at : http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/APPENDIX/IRIGcarrFrequ.htm)

IRIG AM input/output Pinout (via Multi I/O connector)



- IRIG AM In/Out requires IRIG AM Option Card be installed

System Configuration		
System	Orolla VersaSync	SW V1.5.0 (32fa9e7b2b37)
Model	1220-2114	
Serial #	710	
Power Supply	AC 110/220, DC 12V	
Oscillator	OCXO (10ppb)	
Timing Processor		SW V4.0.0 (71e1895f5ac2) / FPGA 90
GNSS Receiver	u-blox MST	SW V3.01 TMI 1.10
HW Slot 1	IRIG AM	NA
Option	OPT-GNSS Multi-GNSS	

➤ Following excerpt from http://manuals.spectracom.com/VSS/Content/VSS/APP/IRIG_AM_OC.htm

There are four dedicated channels for the IRIG AM Option Card: 3 outputs and 1 output. To use these channels for the purpose of IRIG AM, you will need to set the pinout on the multi I/O connector using the Web UI. There are four configurable IRIG AM channels: pins 11 & 12, 13 & 14, 15 & 16, and 17 & 18 (see the chart on the following page for specifics on all pinout configuration options).

- Pins 11 & 12 -- IRIG Output 0
- Pins 13 & 14 -- IRIG Input 0
- Pins 15 & 16 -- IRIG Output 1
- Pins 17 & 18 -- IRIG Output 2

After signing in to the unit, navigate to **MANAGEMENT > NETWORK > Pin Layout**. In the Layout panel, select the plus sign in the upper right corner.

Choose OPTION for both the Signal and the Type Filter, and select the pin set numbers for the pin pair you wish to configure. Click Submit.

The Layout panel should display your new settings. Please note that although the OPTION signal can technically be applied to any pin pair in the Web UI, only pins 11 & 12, 13 & 14, 15 & 16, and 17 & 18 are software supported for the IRIG AM card and will function on that setting.

Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (5V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal -)	19	9 (USB dedicated)	GND
6		GND	20		GND
7	3	1PPS output (10 V)	21		Not connected
8		GND	22		GND
9	4	ASCII output (RS-232)	23		USB D-
10		GND	24		GND
11	5	1PPS input	25		USB D+
12		GND	26		GND
13	6	ASCII input (RS-232)			
14		GND			

Note: IRIG AM input/output (when IRIG AM option card is installed) is restricted to pins 11, 12 or pins 13, 14

IRIG AM configuration

Management -> Network -> Pin Layout

IRIG AM Settings

After configuring the pinout to IRIG AM, it is necessary to configure each output and input with additional settings. In the Web UI, navigate to **INTERFACES -> OPTION CARDS -> Option Board** and then select the necessary signal. Be sure to configure the IRIG outputs and inputs that are under the Option Board header in order to change IRIG AM settings (represented by the orange circle in the image below).



• Pins 11 & 12 - IRIG Output 0
 • Pins 13 & 14 - IRIG Input 0
 • Pins 15 & 16 - IRIG Output 1
 • Pins 17 & 18 - IRIG Output 2

Once you've clicked on the output or input to be configured, a popup window will display the current settings. To manipulate these settings, click on the Edit button for an IRIG AM Output or IRIG AM Input.

A) IRIG AM Input settings

(screenshot with v.1.5.0 installed)

Format: [(A) IRIG A, (B) IRIG B, (G) IRIG G, (N) NASA 36, (E) IRIG E]

Modulation: [(0) IRIG DCLS Only, (1) IRIG AM Only] Please note: the IRIG DCLS only option is non- functional and should not be selected.

Frequency: [(0) No Carrier, (1) 100 Hz, (2) 1 KHz, (3) 10 KHz, (4) 100 KHz, (5) 1 MHz] See previous Note on Format and Frequency

Coded Expression: [(0) BCD TOY, Ctrl Func, Binary Seconds, (1) BCD TOY, Ctrl Func, (2) BCD TOY, (3) BCD TOY, Binary Seconds, (4) BCD TOY/Year, Ctrl Func, Binary Seconds, (5) BCD TOY/Year, Ctrl Func, (6) BCD TOY/Year, (7) BCD TOY/Year, Binary Seconds], where

BCD = Binary Coded Decimal

TOY = Time of Year

Note: the available Coded Expressions options will change based on your previous selections.

Control Function Field: [Fields conform to RCC 200-04, Fields conform to Spectracom format]

Local Clock: [UTC, TAI, GPS] Must be set to the incoming local clock to allow for accurate conversion.

Offset: Account for cable delays or other latencies. The value is entered and displayed in nanoseconds; the available range is -500 to +500 ms.

B) IRIG AM Output settings

(screenshot with v.1.5.0 installed)

IRIG Output 1

IRIG-B121

Signature Control: Output Always Enabled

Format: (B) IRIG B

Modulation: (1) IRIG AM Only

Frequency: (2) 1 KHz

Amplitude: 128

Coded Expression: (1) BCD TOY, CF

Control Function Conformance: RCC 200-04

Timescale: UTC

Offset: 0

Status Submit

Signature control: [Output Always Enabled, Output Enabled in Holdover, Output Disabled in Holdover, and Output Always Disabled]

Format: [(A) IRIG A, (B) IRIG B, (G) IRIG G, (N) NASA 36, (E) IRIG E]

Modulation: [(0) IRIG DCLS Only, (1) IRIG AM Only] Please note: the IRIG DCLS only option is non-functional and should not be selected.

Frequency: [(0) No Carrier, (1) 100 Hz, (2) 1 KHz, (3) 10 KHz, (4) 100 KHz, (5) 1 MHz]

Note on Format and Frequency: For this release, only the following format and frequency combinations are software supported:

IRIG A: 10 KHz

IRIG B: 1 KHz

IRIG G: 100 KHz

NASA 36: 1 KHz

IRIG E: 1 KHz

Amplitude: Must be between 0 and 255 (via digital potentiometer)

“Amplitude” Field (IRIG Output amplitude adjust via digital pot/web browser)

- Refer to online Versasync user guide at:
http://manuals.spectracom.com/VSS/Content/VSS/APP/IRIG_AM_OC.htm?Highlight=irig

Per Ron Dries (17 June 2021):

- DAC range is 0 to 255

- Min to Max amplitude range should be **500mVpp to 10Vpp** (adjustable via the browser)
 - Browser adjustment does not function in software versions prior to 1.5.0 (such as v1.3.1C)
- Was fixed during the 1.5.0 beta testing (Displayed, but apparently does nothing at all in versions prior to 1.5.0)
- I believe Ron D said a DAC value of about “95” sets the amplitude to **3.5Vpp**
- Refer to an IRIG AM output App Note that was created by Eng/Apps team?

Coded Expression: [(0) BCD TOY, Ctrl Func, Binary Seconds, (1) BCD TOY, Ctrl Func, (2) BCD TOY, (3) BCD TOY, Binary Seconds, (4) BCD TOY/Year, Ctrl Func, Binary Seconds, (5) BCD TOY/Year, Ctrl Func, (6) BCD TOY/Year, (7) BCD TOY/Year, Binary Seconds], where:

BCD = Binary Coded Decimal

TOY = Time of Year

Note: the available Coded Expressions options will change based on your previous selections.

Control Function Field: [Fields conform to RCC 200-04, Fields conform to Spectracom format]

Offset: Account for cable delays or other latencies. The value is entered and displayed in nanoseconds; the available range is -500 to +500 ms

***1PPS input

Physical input

Multi I/O connector

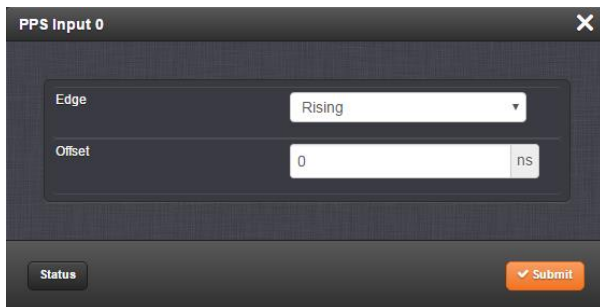


Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (0V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal -)	19	9	GND
6		GND	20	dedicated	GND
7	3	1PPS output (1.8 V)	21		Not connected
8		GND	22		GND
9	4	AOCC output (RS-232)	23		USB D-
10		GND	24		GND
11	5	1PPS input	25		USB D+
12		GND	26		GND
13	6	AOCC input (RS-232)			
14		GND			

1PPS input Configuration

- Refer to online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_PPSin.htm



Edge: [Rising, Falling] The on-time point of the 1PPS input can be configured to be either the rising or falling edge of the 1PPS signal (by default, the rising edge is the on-time point).

Offset: [-500000000 to 500000000 ns = ±0.5 s] Allows to offset the system's 1PPS on-time point, e.g. to compensate for cable delays and other latencies

***Havequick/Stanag input

Physical input

Multi I/O connector



Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal -)	19	9	GND
6		GND	20	USB dedicated	GND
7		5V supply (1.5 V)	21		Not connected
8		GND	22		GND
9	4	ASCII output (RS-232)	23		USB D-
10		GND	24	GND	
11	5	1PPS input	25	USB D+	
12		GND	26	GND	
13	6	ASCII input (RS-232)			
14		GND			

Configuration

- Refer to online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_Setup_In.htm

A screenshot of a web-based configuration interface for 'HQ input 0'. It features three dropdown menus: 'Format' set to 'STANAG 4246 HQ I', 'Timescale' set to 'UTC', and 'Offset' set to '0 ns'. At the bottom, there are 'Status' and 'Submit' buttons.

***ASCII input

Physical input

Multi I/O connector

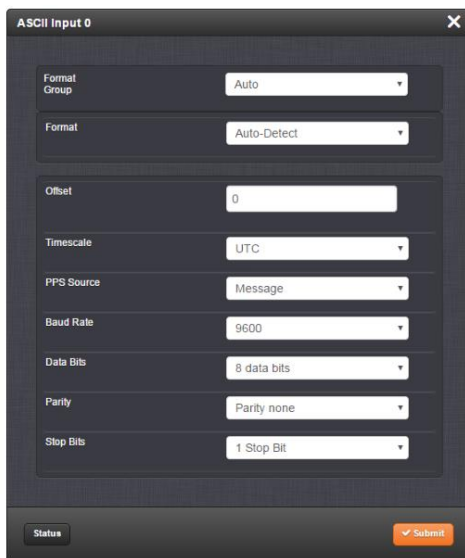


Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (5V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal -)	19	9	GND
6		GND	20	(USB dedicated)	GND
7	3	1PPS output (10 V)	21		Not connected
8		GND	22		GND
9	4	ASCII output (RS-232)	23		USB D-
10		GND	24		GND
11	5	1PPS input	25		USB D+
12		GND	26		GND
13	6	ASCII input (RS-232)			
14		GND			

ASCII Input configuration

- Refer to online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_ASCIIin.htm



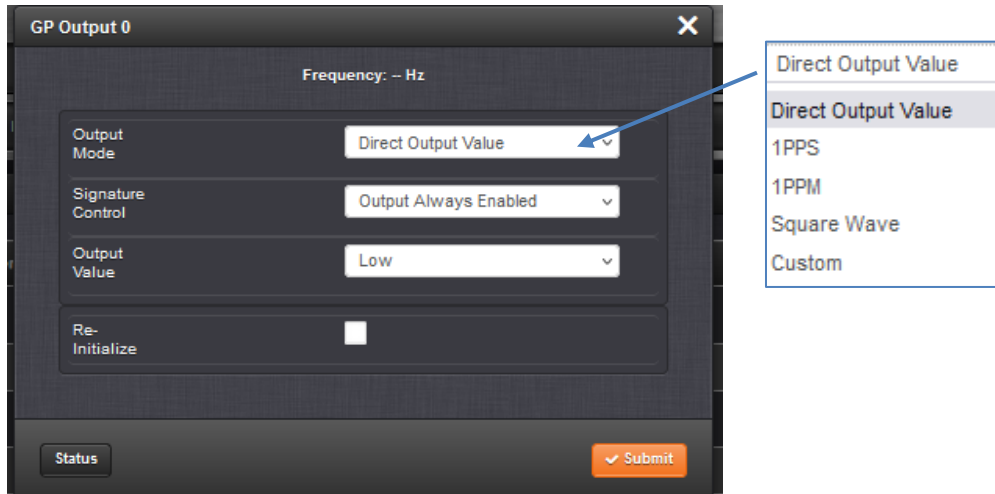
GPI pins (GPIO)

- GPIO functionality added/incorporated in update v1.5.0 (not available in versions 1.4.x and below, including v1.3.1C for IRIG AM Option Card)

After configuring Pin Layout with GPIO pins

Interfaces-> GP output

Screenshot with v1.5.0 installed



***PTP input (PTP Slave)

- Refer to online VersaSync user guide at:
- Refer to "[PTP Master / PTP output](#)" (in this document) for additional input

OUTPUTS

(one or four 10 MHz outputs)



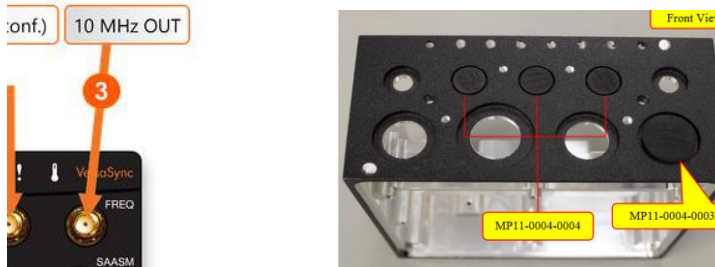
Either **No**, **One** or **Four** SMA 10MHz output(s) is/are installed

- 10 MHz Outputs are on **no**, **one** or **four** SMA connector(s) on front panel
- Versas can be purchased with either only one (1) or with four (4) 10 MHz SMA connectors installed.
 - (4) 10MHz SMA outputs present is referred to as “**10 MHz OUT (special conf.)**” (Special Configuration)

The first of the four digits in the Model Number indicates the 10 MHz configuration installed:

A) 1228-**0**xxx has (1) 10MHz SMA output connector (labeled “Freq”, “10MHz” or “J5”)

Hole plugs installed in J2, J3 and J4 (instead of SMA connectors)



other labeling for 10MHz out (either “J5” or “10MHz”)



B) “Special Conf” (Special Configuration): 1228-**1**xxx has (4) 10MHz outputs (“Freq”, J1, J2 and J3)

- The **ONLY** difference between one 10MHz output and four 10 MHz outputs is the physical hardware difference of three additional SMA output ports being present on the front panel
- Software is exactly the same (instead of the browser settings controlling only one 10 MHz output, the exact same settings simultaneously effect all four outputs (10 MHz outputs are not individually configurable))



C) "Special Conf"(Special Configuration): 1228-**2**xxx has (4)10MHz outputs ("Freq", J1, J2 and J3)

Configuration of 10MHz output(s) (whether just one output, or four SMA outputs installed)

- Refer to the online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/VSS/TIME_MGT/10MHzOutputs.htm?Highlight=10%20mhz
- Can enable or disable Signature Control
- When four 10 MHz outputs are installed, they are not separately configurable.
- The same *Interfaces* -> *10MHz Output 0* page of the browser configures either just the one 10MHz output, or all four 10 MHz outputs (when four are installed).

10 MHz SMA output(s) is/are dedicated/hard-set as 10MHz output(s) only (can't be configured to output any other timing signals, such as 1PPS)

Q Pre-purchase question (4 Aug 2020) We missed that the 1 PPS by default only comes out the breakout cable instead of SMA and were hoping to get at least one SMA configured for 5V 1 PPS out.

A Reply from Keith (4 Aug 2020) Thanks for inquiring about whether its possible for any of the SMA connectors on the VersaSync to be configured to output 1PPS. As described below, this capability isn't available.

Attached for your reference you should find a copy of the VersaSync datasheet. Page 3, and as excerpted below, has two tables associated with the VersaSync outputs.

Per both tables, 1PPS outputs are not available from the SMA connectors (which provide 10 MHz sinewave outputs). The 1PPS outputs are available via the I/O connector (and its associated breakout cable).

Timing Signals

Timing Signal	Coding/Modulation	Input/Output	Connector
GNSS RF	L1 GPS, GLONASS 72 channels, 7.68MHz integrity monitoring Option L1/L2 SAASM	1 input	SMA, 5 VDC power supply to antenna
10 MHz	Sine, 10 dBm	1 output (standard) 4 outputs (optional)	SMA
Pulse/DCLS TTL level	1PPS, xPPS, BRL, HaveQuick, alarm	Max 2 inputs Max 5 outputs	I/O connector
Pulse/DCLS 10 VDC	1PPS, xPPS, BRL, HaveQuick, alarm	Max 1 input Max 1 output	I/O connector
RS232	NMEA 0183, other ASCII ToD-formats	Max 3 inputs Max 3 outputs	I/O connector
RS485	HaveQuick, xPPS	Max 3 inputs Max 4 outputs	I/O connector
NTP over LAN (GbE)	NTP v3, v4, client, server	2	LAN connector
PTP over LAN (GbE)	PTP v1, v2, Master	2	LAN connector

Front Panel Connections

Interface	Type of Data	Connector*
GNSS RF in	GNSS signal	SMA
Power in	DC power	Circular mil-type
Frequency out	10 MHz sine	SMA
Timing in/out	Pulse/DCLS, RS232, RS485, also USB communications	Circular mil-type
GSE	NTP, PTP Navigation messages Monitoring	Circular mil-type
SAASM keyboard	DS101, DS10P	Circular mil-type

*connector pin-outs available in the user manual.

In case you weren't already aware of it, there is an online VersaSync user guide (easily searchable and containing the most up-to-date info on the VersaSync) at: <http://manuals.spectracom.com/VSS/Content/VSS/INTRO/GettingStarted.htm>.

As shown at http://manuals.spectracom.com/VSS/Content/VSS/INTRO/VSS_Interfaces.htm?Highlight=sma, the SMA connectors are only for 10 MHz output.

*1PPS output / xPPS output

- Refer to [**I/O \(input/outputs\) such as USB/Serial](#)
- Refer to online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/SETUP/1PPS_outp_conf.htm

A) 1PPS

Physical connection

“Multi I/O” connector only (Note: 1PPS output is not available via SMA connectors, which are 10MHz only)



Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (5V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal -)	19	9	GND
6		GND	20	(USB dedicated)	GND
7	3	1PPS output (10 V)	21		Not connected
8		GND	22		GND
9	4	ASCII output (RS-232)	23		USB D-
10		GND	24		GND
11	5	1PPS input	25		USB D+
12		GND	26		GND
13	6	ASCII input (RS-232)			
14		GND			

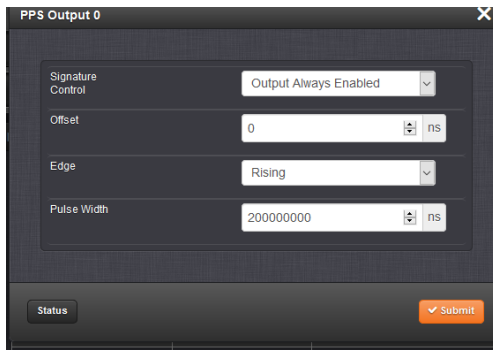
Q What we actually need is a maximum time that we can expect the 1PPS to come after applying power.

This would be for the worst conditions (cold start)

A email from Ron Dries (20 Feb 17 KW) After working with Engineering, the 1PPS will be present about 30 seconds after powering on from a cold start.

1PPS Configuration

Interfaces -> *PPS Output 0* (PPS Output 1)



Pulse Width

[range = 20 to 900000000 ns = 0.0 μ s to 0.9 s]
[default = 200 ms]

B) xPPS (such as “20PPS”)

- xPPS is software-configurable PPS, such as “20PPS”, for example
- xPPS was added in software version 1.0.2.
- 4. per 1.0.2 Release Notes: “[adding xPPS \(configurable PPS, such as 20PPS\)](#)”

Software configuration

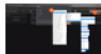
- Refer to example (excerpt below) in VersaSync online user guide:
http://manuals.spectracom.com/VSS/Content/VSS/SETUP/Config_example.htm

Example: Configuring a 20 PPS Output

The instructions below explain how to configure a 20 PPS output signal:

First, assign a GPIO output to an I/O pin pair:

1. In the Web UI, navigate to **MANAGEMENT > NETWORK: Pin Layout**. The **Pin Layout** screen will be displayed.



2. Prior to assigning the new output, identify a pin pair in the Pin Layout table that is not used (Signal = “None”) or not needed. You can **Delete** it, but you may also simply assign the new PPS Output as described below, thus overwriting the existing Input or Output.
3. Add a pin configuration by clicking the PLUS icon in the top-right corner (1). The **Add Pin** window will display.
4. Start with the **Type Filter** drop-down menu (second line in the window) and select **DCLS_TTL**.
5. From the **Signal** drop-down menu, select **GPIO_OUT DCLS_TTL**.
6. From the **Pins** drop-down menu in line 3, select e.g., pins **1,2**.
7. Click **Submit**.
8. In the **Actions** panel, click **Apply Changes**.

Then, configure the settings for the newly created output:

9. Navigate to **INTERFACES > OUTPUTS > General Purpose Output/GP Output 0**. The **GP Output 0** status window will be displayed.
10. Click **Edit**. The **GP Output 0** configuration window will be displayed.
11. Under **General**, set the **Output Mode** to **Square Wave**, and check **Output Enabled**.
12. To configure e.g., a 20 PPS signal, set the **Pulse Width** to 1 000 000 ns, and the **Period** to 50 000 000 ns:



13. Click **Submit**.

***ASCII output

Physical connection

Multi I/O connector

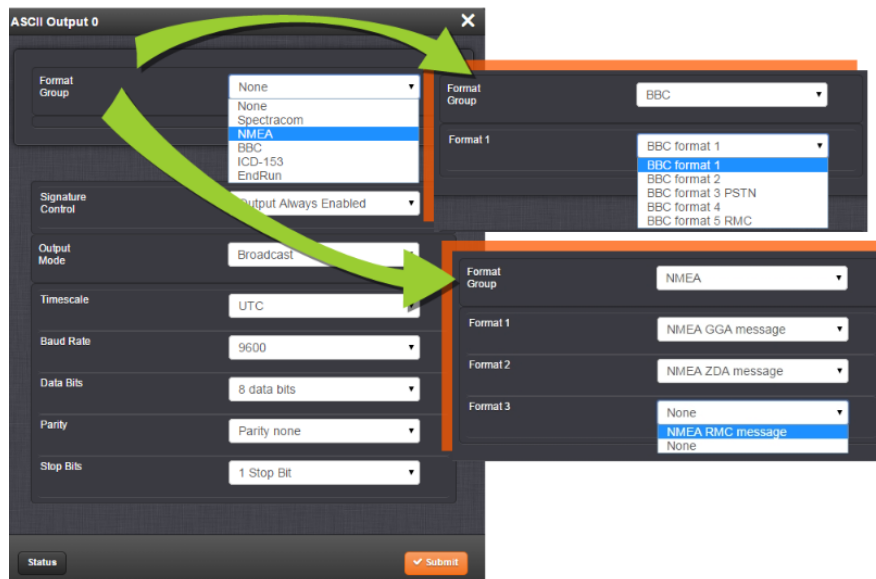


Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	PPS output (5V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal -)	19	9	GND (USB dedicated)
6		GND	20		GND
7	3	PPS output (10 V)	21		Not connected
8		GND	22		GND
9	4	ASCII output (RS-232)	23		USB D-
10		GND	24		GND
11		GND	25		USB D+
12		GND	26		GND
13	6	ASCII input (RS-232)			
14		GND			

ASCII output Configuration

- Refer to online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_ASCIIout.htm



***Havequick/Stanag output

Physical connection

Multi I/O connector

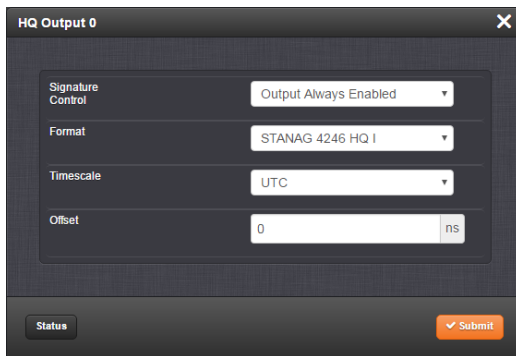


Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal -)	17	8	Have Quick output (RS-485 signal -)
4		GND	18		GND
5	2	Have Quick input (RS-485 signal +)	19		
6		GND	20	dedicated	USB
7	3	1PPS output (I) (V)	21		Not connected
8		GND	22		GND
9	4	ASCI output (RS-232)	23		USB D-
10		GND	24		GND
11	5	1PPS input	25		USB D+
12		GND	26		GND
13	6	ASCI input (RS-232)			
14		GND			

Have quick output Configuration

- Refer to online VersaSync user guide at: http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_StanagHQout.htm



<http://manuals.spectracom.com/VSS/Content/Resources/Images/HQoutput0.png>

GPO Pins (GPIO)

- GPIO functionality incorporated in update v1.5.0 (not available in versions 1.4.x and below, including v1.3.1C for IRIG AM Option Card)
- Signature Control for GPO pin also added in update v1.5.0

PTP Master / PTP output (Eth1 only)

- Engineering VersaSync at: <https://10.10.128.1>
- Refer to online VersaSync user guide “PTP Grandmaster 1204 32”:
http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_PTP.htm

Support of PTP over VLAN

- Refer to VersaSync user guide at: <https://orolia.com/manuals/VSS/Content/VS/Topics/TASKS/VLAN.htm>

Software version limitations on VLAN support of PTP

- Refer to Salesforce Cases such as 292339
- Per Version 1.8.0 (and 1.7.0) release notes: “*PTP over a VLAN interface is not currently functional (from 1.7.0)*”

Note from Keith (excerpted from this case): [Confirm with Engineering \(Will Comley\)](#), but I BELIEVE the note about PTP not working over VLAN is that we do not support VLAN tagging, yet. I believe PTP will still work, as long as they connect the Versa to a switch port that doesn't require VLAN tagging (I believe its referred to as "VLAN-unaware")

ITU-T Standards for PTP (such as SyncE)

- Refer to PTP section of: [.\SecureSync Option Card information.pdf](#)
- Refer also to the “ITU-T” section of [.\CustomerServiceAssistance.pdf](#)

Examples

A) PTP Telecom profile

- G.826x (G.8265.1, G.8275.1/G.8275.2)

B) Frequency sync

- G.826x (G.8260, G.8261, G.8262, G.8263, G.8264, G.8265)

C) Phase/Time Sync

- G.827x (G.8271, G.8272, G.8273, G.8275)

Software version-related

A) PTP4I (PTP for Linux) installed in newer versions of VersaSyncs (in at least 1.5.0 and above) just like 2400 SecureSync versions 1.4.x and above

- Refer to the 2400 SecureSync Assistance doc for more info on ptp4l.
- Adds PTP Slave capability

B) PTP Master availability started in main software version 1.1.5

1. PTP Master only (no PTP Slave functionality, at this time)
2. Multicast mode only (unicast not functional/not tested yet)
3. Available on **eth1 interface only** (as of at least versions 1.4.2 and below (prior to at least Oct 2021)
 - **Per “known issues in v1.4.2 Release Notes: “PTP is currently limited to 1 GB/s networks and to the ETH1 interface”**

PTP Specs

1. **Inputs/Outputs:** (1) Master Port (Available on **eth1 interface only**, as of at least versions 1.2.0 and below)
2. **Signal Type:** Ethernet
3. **Management:** Web UI
4. **Network Speeds:** 100 Mb/s, or 1Gb/s
5. **PTP Version supported:** PTP 1 IEEE (1588-2002) and 2 (IEEE 1588-2008)
6. **PTP Profiles supported:** Default, Telecom, Enterprise
7. **Transmission modes:** Unicast, Multicast [default] (IPv4 and Ethernet)

PTP input (PTP Slave mode) configuration/operation

- Not available in earlier versions (believe all versions prior to v1.5.0)
Email from Pritam to Tony DiFlorio (19 June 2020) I checked this with engineering. The answer is false – don't have PTP slave functionality ported to VersaSync yet, the plan is to support in 1.5.0 release.
- PTP Slave capability was added when PTP4L software replaced masterpiece software (in at least versions 1.5.0? and above)

A) Info below is based on Ptp4l replacing masterpiece software (believe versions 1.5.0 and above)

- **PTP input/output Configuration:** Refer to the online VersaSync user guide at:
https://orolia.com/manuals/VSS/Content/VS/Topics/INTRO/VS_PTP.htm
 - Refer also to “Ptp4l” in the 2400 SecureSync assist doc for additional info on ptp4l software.

Delay Asymmetry for Mean Path Delay customization (Settings -> Network tab)

- Per Keith (15 Nov 2022) Delay Asymmetry is being added in 2400 SecureSync version 1.6.0. As of the current VersaSync version of 1.5.0, this new configuration has not yet been added to VersaSyncs. However, the VersaSync user guide was updated at the same time as the 2400 SecureSync guide, to show this new configuration which is about to be available in only 2400 SecureSyncs. It will likely one day be added to VersaSyncs in a future, post 1.5.0 VersaSync update.

PTP Output configuration/operation

- Ptp4l (PTP for linux) software replacing masterpiece software (starting in software versions **1.5.0?** and above) implemented many changes to PTP operation
 - Refer also to “**Ptp4l**” in the 2400 SecureSync assist doc for additional info

A) Info below is based on ptp4l (ptp for linux”, which replaced masterpiece starting in versions 1.5.0? and above)

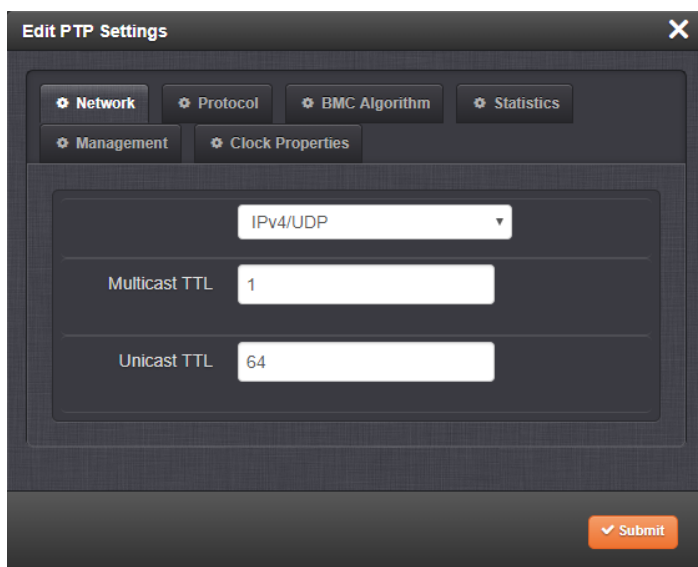
PTP output Configuration (very similar to 2400 SecureSyncs at versions 1.4x and above: Refer to the online VersaSync user guide at: https://orolia.com/manuals/VSS/Content/VS/Topics/INTRO/VS_PTP.htm)



B) Info below is based on PTP output using “masterpiece” in earlier versions of VersaSync (before ptp4l was added,1.5.0?)

PTP output web browser page/tabs (versions 1.4.0 and below)

Management -> *PTP Setup* page of the browser



The PTP Tabs

Network tab

1. **Protocol:** [IPv4/UDP, Ethernet] Selects the transport protocol used for PTP packets. If Ethernet is chosen, IP address data will be shown below. If IPv4/UDP (User Datagram Protocol) is chosen, Mac addresses will be displayed.
2. **Multicast Ttl:** [1 through 255] Time-to-live (packet lifespan) — Sets the TTL field for PTP packets except for Peer-to-Peer packets for which TTL is forced to 1 as specified in IEEE Std 1588-2008 Annex D.3.
3. **Unicast Ttl:** [64] Time to live for Unicast packets.

Protocol tab

1. **PTP Version:** [1, 2] Select Version 1 or Version 2.
2. **Domain:** [1 through 127] Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1
3. **Sync Rate:** The rate at which Sync messages are sent, in packets per second. [1 = 1 packet/sec.; 2 = 2 packets/sec.; 0.5 = 1 packet/2 sec.]
4. **Communication Mode:** Select multicast, hybrid, or unicast mode.
5. **Announce Rate:** [see Sync Rate above] The rate at which Announce messages are sent, in packets per second.
6. **Delay Request Rate:** Interval between request messages sent by the slave to the master.

BMC Algorithm tab

1. **[ENABLE/DISABLE]**
2. **Announce Receipt Timeout Intervals:** [4] The number of Announce Intervals that must pass without receiving an announce message before the node decides that the Master sending the Announce Messages is no longer present on the network.

Statistics tab

1. **Cleanup interval**, s
2. **Update interval**, s

Management tab

1. **Resp State**: [ON/OFF] Enable/disable Management Responses.
2. **Req State**: [ON/OFF] Enable/disable Management Requests.
3. **Req Rate**: [0.2 = one request every five seconds] Request rate in seconds for PTP Management messages.

Clock Properties tab

1. **Grandmaster Priority 1**: [0 to 255] (0 is highest priority. Default is 128 for both priority values. This is usually the priority value that a Slave is set to.) See IEEE 1588-2008, Section 8.10.1, 8.10.2.
2. **Grandmaster Priority 2**: [0 to 255] (0 is highest priority. Default is 128 for both priority values. This is usually the priority value that a Slave is set to.) See IEEE 1588-2008, Section 8.10.1, 8.10.2.

PTP Status panel

The PTP Status panel provides the following status information:

- **Interface Name:** The Ethernet port currently in use (eth 0, or eth1, but not both).
 - **Mode:** [Currently, the only mode supported is Master Only]
 - **Best Master Clock Algorithm:** Indicates if the BMC algorithm is turned ON or OFF (see [BMC Algorithm tab \(Best Master Clock\)](#))
 - **TwoStep:** Indicates the clock mode; PTP has two ways to transmit the initial T1 timestamp of the Sync packet transmission from the Master to the Slave:
 1. **One-Step Master:** The Sync packet is timestamped, then the timestamp is inserted into the Sync packet in real-time, as it is transmitted
 2. **Two-Step Master:** The Sync packet is timestamped, but the timestamp value in the Sync packet is ignored. The actual T1 value is transmitted in a "Follow-Up" packet after the Sync packet.
- Note:** One mode or the other must be selected. The default mode is one-step.
- **Unicast:** Indicates if Unicast is turned ON or OFF. If OFF, VersaSync will not respond to Unicast Delay Requests. (It will respond to Multicast requests, though.)
 - **Negotiation:** Indicates if Unicast Negotiation is turned ON or OFF. If OFF, VersaSync will not respond to Negotiation Requests, i.e. there will be no Unicast Sync Messages.
 - **Domain:** [0 to 255; 128-255 are reserved, as per standards] Indicates the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1.
 - **Transport Protocol:** Indicates if IPv4 or Ethernet is currently used.
 - **Unicast IP Address:** Indicates the interface IP address.

The "PTP Statistics" Panel

VersaSync listens to all PTP traffic on the network. In order to filter statistics to be displayed, the PTP Statistics panel allows you to select a specific PTP node from all the detected nodes on the network, using the Address field.

Note: Note that 0.0.0.0 refers to your local host address, in other words your VersaSync unit.

Select the Message Type for which you would like detailed statistics to be displayed in the panel below.

Note: The choice of Message Types may vary, depending on the selected PTP node.

The Packet Message Statistics Panel

- This panel provides statistics for the Message Type and the PTP node selected in the panel above:

All statistics shown are based on the traffic that is detectable by VersaSync, i.e. in a Unicast environment, VersaSync may only detect traffic that is addressed to it, based on switch configuration.

- **Clock Identity:** [e.g., "a0:36:9f:ff:fe:37:b9:5d"] What is this hex address?
- **Domain:** Domain number of the selected PTP node.
- **Unicast:** [0,1] OFF or ON (1)
- **Message Type:**
 - Management
 - Sync
 - Follow Up
 - Delay Response
 - Delay Request
 - Announce
- **First Time:** [e.g., "2016-08-12 12:23:15"] The first time a packet was received.
- **Last Time:** [e.g., "2016-08-12 18:19:15"] The last time a packet was received.
- **Count:** [e.g., "1336"] Indicates how many times the selected message has been detected.
- **Average Rate:** [e.g., "0.0624986091344933"] Indicates how often the selected message has been detected (in seconds e.g., "1.0" would mean once every second)
- 1. **Missing Packets:** [e.g., "1023961"] Indicates how many packets of the selected message type have been missed.
- 2. **Steps Removed:** The number of communication paths traversed between the local clock and the grandmaster clock.
 - 1 = a single path was traversed
 - 2 = two paths were traversed (there was a boundary clock in the middle).
- 3. **Mean Path Delay:** Slave's calculation of path delay between itself and the Master.
- 4. **Offset From Master:** Slave's calculation how far off its time is (takes into account Mean Path Delay calculations). When selecting a PTP Slave, and the Management message type, this field will be populated with data provided by the Management interface.

PTP output configuration

- Refer also to the VersaSync online manual ("PTP Grandmaster 1204 32" section)
http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_PTP.htm?Highlight=ptp

Choose which device to report data in area below

The Packet Message Statistics Panel

Clock Identity	00:0c:ec:ffe:0c:00:08
Domain	1
Unicast	0
Message Type	Sync
First Time	1970-01-07 02:26:56
Last Time	1970-01-07 02:29:45
Count	170
Average Rate	1.00000045452683
Missing Packets	0
Steps Removed	0
Mean Path Delay	0
Offset From Master	0

Packet Message Statistics Panel (bottom right)

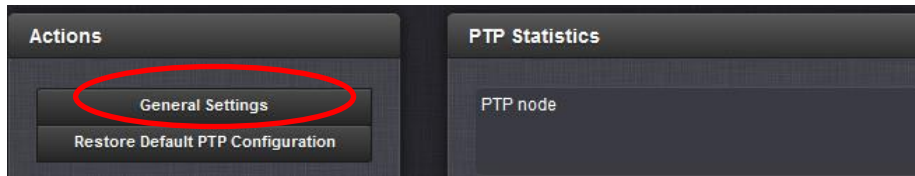
Bottom-right panel provides statistics for the Message Type and the PTP node selected in the top above:

All statistics shown are based on the traffic that is detectable by VersaSync, i.e. in a Unicast environment, VersaSync may only detect traffic that is addressed to it, based on switch configuration.

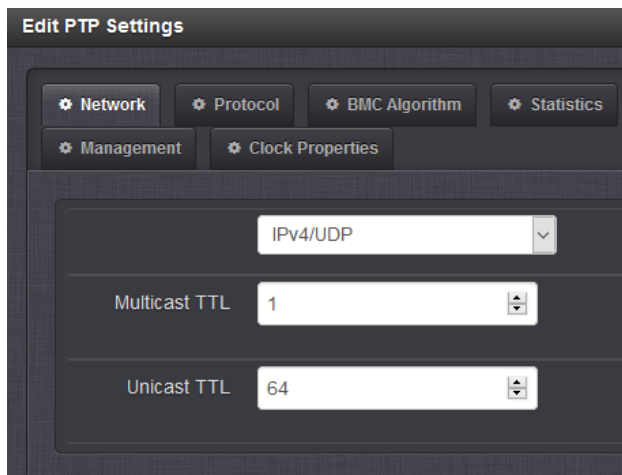
- **Clock Identity:** [e.g., "a0:36:9f:ff:fe:37:b9:5d"] What is this hex address?
- **Domain: Domain number of the selected PTP node.**
- **Unicast:** [0,1] OFF or ON (1)
- **Message Type:**
 - Management
 - Sync
 - Follow Up
 - Delay Response
 - Delay Request
 - Announce
- **First Time:** [e.g., "2016-08-12 12:23:15"] The first time a packet was received.
- **Last Time:** [e.g., "2016-08-12 18:19:15"] The last time a packet was received.
- **Count:** [e.g., "1336"] Indicates how many times the selected message has been detected.
- **Average Rate:** [e.g., "0.0624986091344933"] Indicates how often the selected message has been detected (in seconds e.g., "1.0" would mean once every second)
- **Missing Packets:** [e.g., "1023961"] Indicates how many packets of the selected message type have been missed.
- **Steps Removed:** The number of communication paths traversed between the local

“General Settings” pop-up window (button In upper-left corner)

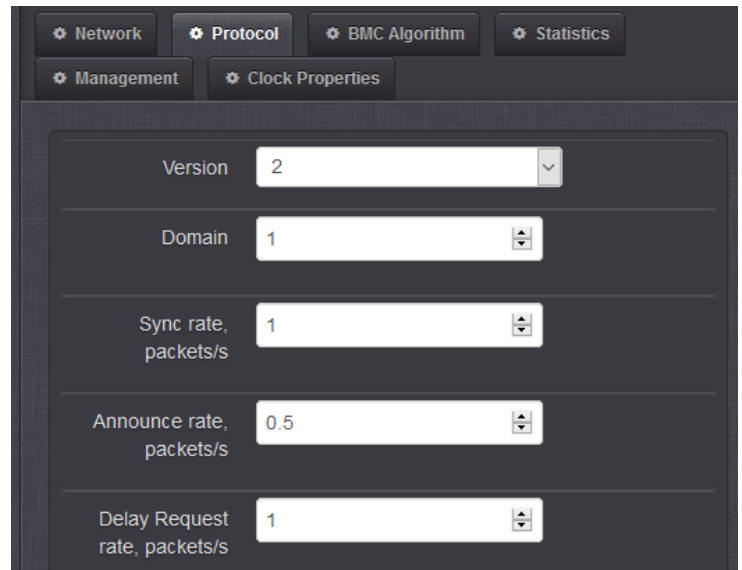
➤ Consists of several tabs



(Network tab) (TTL values)



(Protocol tab) (domain, Sync/Announce rates)



Unicast Mode (not yet available): This is a Point-to-Point transmission mode between two PT Clocks by means of the unique IP address assigned to each PTP Clock.

Note: The Unicast mode is only implemented for the following PTP packets: **Announce**, **Sync** and **Follow-Up**, **Delay_Req** and **Delay_Resp**.

The Unicast mode is activated at the initiative of the Slaves. Each Slave, which wants to run in Unicast mode, shall first negotiate Unicast contracts with the Master.

When Unicast is selected, the following options will be displayed instead of Multicast Ttl.:

Unicast Mac address: [00:00:00:00:00:00]

Unicast Ttl: [64] Time to live for Unicast packets.

Negotiation: If ON, the following fields will be displayed:

- **Duration Sync:** [600] Duration in seconds for Sync contract
- **Duration Announce:** [600] Duration in seconds for Announce contract
- **Duration Delay Req:** [600] Duration in seconds for Delay Request contract
- **Renewal Margin:** [5] Seconds before end of contract before a new message is requested
- **Request Interval:** [1] Interval in seconds, at which the request will be repeated before it times out. Example: if the Margin is set to 5 seconds, and the interval is set to 1 second, the request will be repeated 5 times.
- **Multicast Ttl:** [1] Time to live for contract negotiation management messages

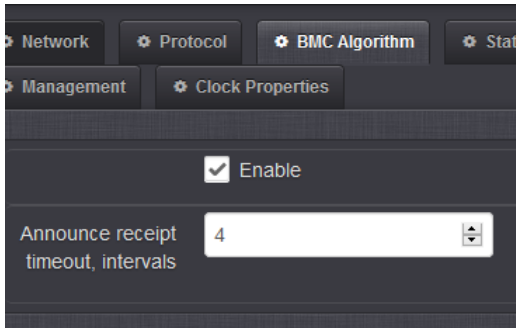
Twostep (not yet available) : The Sync packet is timestamped, but the timestamp value in the Sync packet is ignored. The actual T1 value is transmitted in a "Follow-Up" packet after the Sync packet.

Note: PTP Masters must select one mode or the other to operate in. The **default** mode is **one-step**.

Sync Rate: The rate at which Sync messages are sent, in packets per second. [1 = 1 packet/sec.; 2 = 2 packets/sec.; 0.5 = 1 packet/2 sec.]

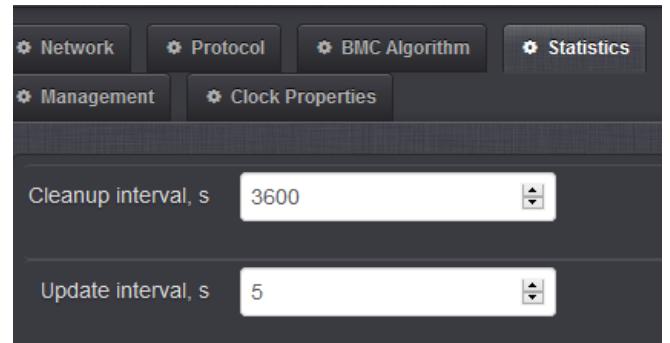
Announce Rate: [see Sync Rate above] The rate at which Announce messages are sent, in packets per second.

(BMC Algorithm tab)



(Statistics tab)

Note: If VersaSync does not detect any PTP traffic, the PTP screen will display 'No status available' message, instead of data.



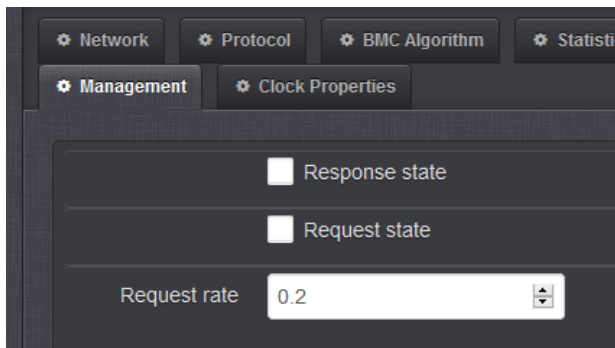
“Enable” checkbox

Selected: In Slave mode, if more than one master clocks are detected, the algorithm will cause VersaSync to use the superior of the two masters. The inferior one will become passive. (slave mode not currently available)

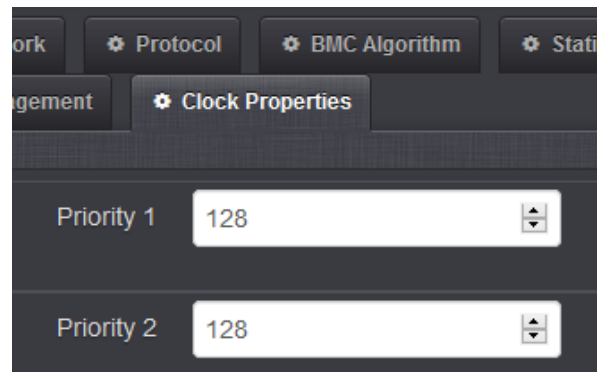
Not selected: In Multicast mode, competing master clocks will be allowed to send out their timing packets.

Announce Receipt Timeout Intervals: [4] The number of Announce Intervals that must pass without receiving an announce message before the node decides that the Master sending the Announce Messages is no longer present on the network.

(Management tab) (enable/disable Management Messages)



(Clock Properties tab) (configure Priority values)



Response State: Enable/disable Management Responses.

Request State: Enable/disable Management Requests.

Request Rate: [0.2 = one request every five seconds] Request rate in seconds for PTP Management messages.

“PTP Status” section of the [PTP](#) -> [Setup](#) page

The image shows a configuration interface for Precision Time Protocol (PTP). It is divided into two main sections: "PTP Services" and "PTP Status".

PTP Services

- PTP: ON

PTP Status

- Transport: IPv4/UDP
- 2 Step: On
- Domain: 1
- Best Master Clock Algorithm: On
- Unicast: Off
- Current IP Address: 10.10.128.62

Software fixes/Known issues with PTP output (PTP operations) prior to version 1.5.0

- Refer also to VersaSync Release Notes: <I:\Customer Service\PSB, PSP software updates\Versaync>

PTP changes in update v1.4.1

- Repaired a problem with PTP not working when both network interfaces were connected to the same subnet.
- Fixed a problem with the PTP ceasing operation under certain conditions.
- Corrected an intermittent error with some PTP users experiencing a one-second offset.

1) All PTP packets (such as Announce and Sync messages) stop outputting upon loss of PTP Slaves

- Refer to Salesforce Case 221606 (issue reported Jan 2020)
- Refer to JIRA VPNT-517 (as well as VPNT-504 and VPNT-518)
- Observed in Version 1.3.1K
- Requires reboot to start outputting packets again.

Per Denis Reilly (4 March 2020) I saw a similar issue when working on VPNT-504 and VPNT-518, when the PTP master in the Versa seemed to stop working if communication wasn't coming into it. It may have been caused by the same commit that we backed out to fix VPNT-518. It's very possible that this will fix the issue for the customer.

I think the original customer issue was entered as VPNT-517, so if the new release fixes that then we should close it.

2) Periodic 1 second offset spikes

- Refer to Salesforce Case 208874 (issue reported Sept 2019)
- Refer to JIRA VPNT-504 (<https://spectracom.atlassian.net/browse/VPNT-504>)
- Observed in versions 1.3.1D and 1.3.1K

Email from Pritam (6 Feb 2020) Hi Ryan and Team, When this case was escalated to Apps team, initially we were not able to recreate the issue of 1 sec offset. However later after working with customer and engineering we were able to reproduce this in our lab. Jodi updated these information in the case 208874.

Denis and/or I can work with Julien and team as necessary so that we can add fix in our next release.

Reply from Ryan Johnson: Even though it has been duplicated, we don't understand yet how this is happening, so we don't have a fix readily available. We'll need to determine the cause of the problem first before knowing when/how a patch could be delivered. Denis says he has a few theories but those will need to be validated first.

3) Software issue generates zero-byte management messages

Email from Denis Reilly (9 Dec 2019) You might also want to advise the customer to turn off the management messages , or at the very least, turn "Request Peer Information" off. We have a bug that generates zero-byte management messages, and his linuxptp doesn't like that.

4) PTP stops responding after ~10 minutes

- Refer to Salesforce Case 184893 (case started ~Feb 2019)

- “VersaSync’s stopping PTP traffic after running for about 10 minutes”.
- Initially reported with **v1.1.5** installed, but also observed with **v1.3.1d** installed.

** Chrony NTP output (“NTP server”)

- NTP functionality in VersaSyncs (similar to Model 1232 Velasyncs) is provided by Chrony– not NTP implementation
- Chrony has replaced NTP software in newer versions of linux
- Refer to “**Chrony**” in: [..\CustomerServiceAssistance.pdf](#)
- Refer especially to: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-understanding_chrony_and_its_configuration
or other sites such as:
<https://chrony.tuxfamily.org/> and http://docs.fedoraproject.org/en-US/Fedora/18/html/System_Administrators_Guide/chap-Configuring_NTP_Using_the_chrony_Suite.html
- Chrony is apparently replacing NTP (per http://docs.fedoraproject.org/en-US/Fedora/18/html/System_Administrators_Guide/chap-Configuring_NTP_Using_the_chrony_Suite.html) “*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.

What is Chrony NTP:

Below is from <https://chrony.tuxfamily.org/>

Chrony is a versatile implementation of the Network Time Protocol (NTP). It can synchronise 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.

It is designed to perform well in a wide range of conditions, including intermittent network connections, heavily congested networks, changing temperatures (ordinary computer clocks are sensitive to temperature), and systems that do not run continuously, or run on a virtual machine.

Typical accuracy between two machines synchronized over the Internet is within a few milliseconds; on a LAN, accuracy is typically in tens of microseconds. With hardware timestamping, or a hardware reference clock, sub-microsecond accuracy may be possible.

Two programs are included in chrony, **chronyd** is a daemon that can be started at boot time and **chronyc** is a command-line interface program which can be used to monitor **chronyd**'s performance and to change various operating parameters whilst it is running.

Which ports can serve NTP

- NTP is available on all network ports

Chrony NTP versions supported

- VersaSync supports all versions of NTP (1 through 4)
- No special configuration is required for version selection

NTP Expert mode (not currently available)

- not available in at least versions 1.1.2 (~June 2019) and below

NTP peering (Stratum 2 operation)

- **NTP peering is not “operational” in at least version 1.3k (~June 2019) and below**

VelaSync Update version 1.1.2: Per the Model 1232 version 1.1.2 Release Notes “**Fixed an issue preventing Stratum 2 NTP operation without an active timing reference.**”

Per conversation with Denis R (2 July 2019): In previous Model 1232 VelaSync software versions 1.1.0 and 1.1.1, the TSync board inside the VelaSync was always being used by Chrony as a valid input reference (whether the TSync-PCIe board was synced to GPS, in Holdover mode, or if it was not in sync/not in Holdover). This was causing Chrony NTP in the VelaSync to always be a Stratum 1 time sever! It wouldn't switch to Stratum 16 upon loss of all valid input references.

Since GPS input to Chrony takes priority over NTP peers/NTP servers, TSync input always being considered by Chrony to be a valid input in versions 1.1.0 and 1.1.1, it would never switch to other NTP peers/servers as its selected reference ("TSync GPS is always valid, so why should I switch to an NTP input").

Known issues with NTP output

1. NTP works for a while and then stops outputting responses

- Per discussion with Ron Dries (8 March 2019) there was a known issue in earlier versions (such as around 1.3.1) where NTP would work for a while and then stop outputting packets
- per Ron, this was addressed in the 1.3.x series of updates (1.3.1a. 1.3.1b. 1.3.1c. 1.3.1d with at least 1.3.1d no longer observing this condition.
- Customers reporting this condition should first try updating the software to the latest version to see if it's still observed.

Checking the status of Chrony (**chronyc** CLI commands)

- Refer to: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-using_chrony

A) Using **ntpq** cli commands

ntpq -p and **ntpq -pn** (NTPQ peers CLI commands to check NTP Peers/NTP Servers)

- ntpq commands are still available with VersaSyncs (even though this product is using Chrony instead of ntp)

B) Using **chronyc** CLI command for checking Chrony Sources

Note: use **shift + C** to exit out of chronyc (to go back to the standard command prompt)

1. At the CLI command prompt, type **chronyc**<enter>
2. Then, at the chronyc prompt, type **sources -v**<enter> (where the optional "-v" adds additional details)
(or just type **sourcestate**, if already at the chronyc prompt)

The **sources** command displays information about the current time sources that chronyd is accessing. The optional argument -v can be specified, meaning verbose. In this case, extra caption lines are shown as a reminder of the meanings of the columns.

Example response below

```
~]$ chronyc sources
      210 Number of sources = 3
MS Name/IP address         Stratum Poll Reach LastRx Last sample
```

```

=====
#* GPS0                0   4   377   11  -479ns [ -621ns] +/-  134ns
^? a.b.c               2   6   377   23  -923us [ -924us] +/-   43ms
^+ d.e.f               1   6   377   21 -2629us [-2619us] +/-   86ms

```

The columns of the above response are as follows:

M This indicates the mode of the source. ^ means a server, = means a peer and # indicates a locally connected reference clock.

S This column indicates the state of the sources. “*” indicates the source to which chronyd is currently synchronized. “+” indicates acceptable sources which are combined with the selected source. “-” indicates acceptable sources which are excluded by the combining algorithm. “?” indicates sources to which connectivity has been lost or whose packets do not pass all tests. “x” indicates a clock which chronyd thinks is a *false ticker* (its time is inconsistent with a majority of other sources). “~” indicates a source whose time appears to have too much variability. The “?” condition is also shown at start-up, until at least 3 samples have been gathered from it.

Name/IP address This shows the name or the IP address of the source, or reference ID for reference clock.

Stratum This shows the stratum of the source, as reported in its most recently received sample. Stratum 1 indicates a computer with a locally attached reference clock. A computer that is synchronized to a stratum 1 computer is at stratum 2. A computer that is synchronized to a stratum 2 computer is at stratum 3, and so on.

Poll This shows the rate at which the source is being polled, as a base-2 logarithm of the interval in seconds. Thus, a value of 6 would indicate that a measurement is being made every 64 seconds. chronyd automatically varies the polling rate in response to prevailing conditions.

Reach This shows the source’s reach register printed as an octal number. The register has 8 bits and is updated on every received or missed packet from the source. A value of 377 indicates that a valid reply was received for all of the last eight transmissions.

LastRx This column shows how long ago the last sample was received from the source. This is normally in seconds. The letters m, h, d or y indicate minutes, hours, days or years. A value of 10 years indicates there were no samples received from this source yet.

Last sample This column shows the offset between the local clock and the source at the last measurement. The number in the square brackets shows the actual measured offset. This may be suffixed by ns (indicating nanoseconds), us (indicating microseconds), ms (indicating milliseconds), or s (indicating seconds). The number to the left of the square brackets shows the original measurement, adjusted to allow for any slews applied to the local clock since. The number following the +/- indicator shows the margin of error in the measurement. Positive offsets indicate that the local clock is ahead of the source.

Using `chronyc` CLI command for checking Chrony Source Statistics

Note: Use **shift + C** to exit out of chronyc (to go back to the standard command prompt)

1. At the CLI command prompt, type `chronyc<enter>`
2. Then, at the chronyc prompt, type `sourcestats -v <enter>` (where the optional “-v” adds additional details) (or just type `sourcestats`, if already at the chronyc prompt)

The `sourcestats` command displays information about the drift rate and offset estimation process for each of the sources currently being examined by `chronyd`. The optional argument `-v` can be specified, meaning verbose. In this case, extra caption lines are shown as a reminder of the meanings of the columns

Example response below

```
~]$ chronyc sourcestats
210 Number of sources = 1
Name/IP Address          NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
=====
abc.def.ghi              11   5   46m   -0.001     0.045      1us    25us
```

The columns are as follows:

Name/IP address This is the name or IP address of the NTP server (or peer) or reference ID of the reference clock to which the rest of the line relates.

NP This is the number of sample points currently being retained for the server. The drift rate and current offset are estimated by performing a linear regression through these points.

NR This is the number of runs of residuals having the same sign following the last regression. If this number starts to become too small relative to the number of samples, it indicates that a straight line is no longer a good fit to the data. If the number of runs is too low, `chronyd` discards older samples and re-runs the regression until the number of runs becomes acceptable.

Span This is the interval between the oldest and newest samples. If no unit is shown the value is in seconds. In the example, the interval is 46 minutes.

Frequency This is the estimated residual frequency for the server, in parts per million. In this case, the computer's clock is estimated to be running 1 part in 10^9 slow relative to the server.

Freq Skew This is the estimated error bounds on Freq (again in parts per million).

Offset This is the estimated offset of the source.

Std Dev This is the estimated sample standard deviation.

Manually Adjusting the System Clock ??

To step the system clock immediately, bypassing any adjustments in progress by slewing, issue the following command as root:

```
~]# chronyc makestep
```

If the `rtcfile` directive is used, the real-time clock should not be manually adjusted. Random adjustments would interfere with **chrony**'s need to measure the rate at which the real-time clock drifts.

***ASCII Serial outputs

NMEA outputs (GGA/RMC/ZDA)

NMEA Fields: Magnetic variation/speed over ground/course over ground

Certain fields in the output data streams (Magnetic variation/speed over ground/course over ground) contain a “constant 0” (instead of actual data)

- Refer to Salesforce Cases such as 228837 and 261559

Email from Ron Dries (2 April 2020) (pertaining to Salesforce Case 228837) We do not populate magnetic variation, speed over ground or course over ground. So as long as you are getting correct values for latitude, longitude and altitude, the VersaSync's ASCII output is connected correctly to the other system.

Related follow-up question from a different customer (per Salesforce Case 261559): Is it possible to input magnetic variation, to be outputted in the data streams

- Refer to Salesforce Case 261559 (April 2021)
 - Refer to JIRA ticket VPNT-656 (April 2021)
5. Keith believes this is a “feature request” for VersaSyncs (confirming with Engineering)
6. Appears to also be directly related to an earlier OGSi opportunity with same customer, for VersaPNTs...

Email from Matt Loomis to Trevor Bertrand (6 April 2021) Please jump on this after the JYC webinar. This is RSG Aero that wanted to add MagVar to VersaPNT.. ODS (Tyler) was involved on this early last year.. Covid postponed. [RSG AeroDesign \(L3\) - \[Morroco\] HELRAS System 2x VersaPNT + NRE MagVar | Salesforce](#)

New feature: NMEA-over-UDP functionality

Version 1.8.0 update (~Dec 2022) added NMEA-over-UDP functionality. For more information, see the App Note at: <https://www.rolia.com/document/nmea-over-udp/>.

Note: multicast frames can only be sent on Eth0 (not Eth1)

Stanag/HaveQuick output

Refer to online SecureSync user guide:

http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_StanagHQout.htm

Configuration

Interfaces -> Havequick output

Screenshot from v1.1.5

HQ Output 0 ✕

Signature Control ▼

Format ▼

Timescale ▼

Offset ▼ ns

Status ✓ Submit

***USB/Serial interface for CLI connection / USB Driver

- Allows a serial to USB connection via a virtual com port
- Compliant with USB 2.0 specification.

USB driver

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\VersaSync\USB driver>
- UART IC in the VersaSync is an FT232R
- Driver is automatically downloaded if PC can access the Internet
- If the device is isolated from the Internet, the driver can be downloaded at no cost from either:
 1. **The VersaSync online user manual:**
<http://manuals.spectracom.com/VSS/Content/VSS/SETUP/QuickStart.htm> under “USB driver”.
 2. **The FTDI website** (indicated on page 2 of their data sheet):
<http://www.ftdichip.com/Documents/InstallGuides.htm>

Serial connections

- 115,000 baud, 8, 1, N

Email from Mark McGregor (8 Feb 17) The USB on VersaSync is the Linux console and CLI interface.

The setup of the virtual COM port on the user terminal program is 115k, N, 8, 1.

If the customer cycles power to the VersaSync the Virtual COM part will come up new as well. The virtual COM port has to sometimes be re-selected in the terminal program because the COM port number changed. If the virtual COM part does not change, the terminal program might have to disconnect and re-connect to get the command line going.

When the unit is up and running it will have the Spectracom login.

I think that the admin or spadadmin login will work, but I am not sure because it has been awhile. I know I used spfactory successfully, The unit does DHCP, so the command line Linux command “ifconfig” might be needed to get the IP address to bring up the web UI.

CLI interface (Command Line Interface)

- Refer to the online VersaSync user guide:
http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=cli
- Our CLI is proprietary. Orolia/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

- VersaSyncs have GNU Bash installed
- The CLI command to obtain the Bash version is: **bash -version** (“dash, dash” before “version”).

VersaSync CLI commands

- Refer to online VersaSync user guide:

http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=cli

Command	Description
clean	Restores VersaSync configuration to factory defaults and reboots
cleanhalt	Restores VersaSync configuration to factory defaults and halts
clearlogs	Clears all logs
clearstats	Clears all statistical data (NTP, and oscillator/disciplining)
dateget	Displays current date (for example, 15 APR 2015)
dateset	Used to set the current date
defcert	Used to create a new Spectracom self-signed SSL certificate for HTTPS in case of expiration of the original certificate
dhcp4get	Displays whether DHCP is enabled
dhcp4set	Used to enable or disable DHCP
dns4get	Displays the configured DNS servers
dns4set	Used to configure the DNS servers
dhcp6get	Displays whether DHCPv6 is enabled
dhcp6set	Used to enable or disable DHCPv6
doynet	Used to obtain the current Day of Year
doynset	Used to set the current Day of Year
gpsdop	Displays GNSS receiver positional accuracy estimates
gpsdserviceportget	Displays the GPSD service port
gpsdserviceportset	Sets the GPSD service port
gpsinfo	Applicable to SAASM-equipped VersaSync units only
gpsloc	Displays GNSS latitude, longitude and antenna height
gpsmdl	Displays the GNSS Manufacturer and Model
gpsstat	Displays GNSS satellites tracked and maximum signal strength being received
gw4get	Displays configured IPv4 gateway addresses
gw4set	Used to configure the IPv4 gateway addresses
gw6get	Displays configured IPv6 gateway address
gw6set	Used to configure the IPv6 gateway address
halt	Used to Halt the system for shutdown
helpcli	Provides list of available commands and syntax
hostget	Displays the DNS hostname
hostset	Sets the DNS hostname
hotstart	Initiate a hot start operation on the SAASM GPS receiver
ip4get	Displays IPv4 Ethernet port settings information (IP address net mask and gateway)
ip4set	Used to set IPv4 Ethernet port settings information (IP address net mask and gateway)
ip6add	Used to add IPv6 Ethernet port settings information (IP address net mask and gateway)
ip6del	Used to delete IPv6 IP address
ip6get	Used to obtain the IPv6 IP address
iptables	See Network Services for more information.
licenses	Displays configured licenses installed (if any)
list	Outputs a list of commands
loadconf	Restore a saved configuration and reboot
localget	Used to obtain the configured local clock
locallist	Used to display local clocks
localset	Used to configure local clocks
model	Displays the Serial Number of the unit
net	Displays network status
netnum	Displays the number of general-purpose network interfaces
net4	Displays IPv4 network status
net6	Displays IPv6 network status
options	Displays configured options installed (if any)

Command	Description
oscget	Displays the installed system oscillator
portget	Display whether network port is enabled (for example, "portget ETH2")
portset	Enable or disable a network port: "portset x on" where "x" is the port number (for example, "ETH2") "portset X off" [NOTE: Available since Web UI Revision no. 5.1.2]
portstate	Display the current state for a network port
ppsctrl	Enable/disable individual 1PPS output signals
priorset	Sets the priority of an entry in the reference priority table
radius setretry	<value> Sets how many radius login retries will be attempted
radius getretry	<value> Gets the number of radius login retry attempts
radius server list	Lists radius servers
radius server add	<host> <port> <key> <timeout> Adds radius server
radius server del	<id> Deletes radius server number <id>
reboot	Used to warm-boot the unit without having to disconnect or reconnect power
reftable	Displays reference priority table
release4	Used with DHCP to release the IPv4 address
release6	Used with DHCPv6 to release the IPv6 address
renew4	Used with DHCP to renew the assigned IPv4 address
renew6	Used with DHCPv6 to renew the assigned IPv6 address
resetpw	Resets the administrator account (spadmin) password back to the default value "admin123"
routes4	Displays the current IPv4 routing table(s)
routes6	Displays the current IPv6 routing table(s)
rt4add	Adds an IPv4 static route
rt4del	Deletes an IPv4 static route
rt4get	Displays the configured IPv4 static routes
rt6add	Adds an IPv6 static route
rt6del	Deletes an IPv6 static route
rt6get	Displays the configured IPv6 static routes
saveconf	Generate archive of current configuration
saveolog	Generate archive of all log files
scaleget	Displays configured system timescale
scaleset	Used to configure the system timescale
services	Displays the state of services (enabled/disabled)
servget	Displays the state of individual services
servset	Enable or disable specific services
slaacget	Displays whether SLAAC is enabled
slaacset	Used to enable or disable SLAAC
stateset	Enable or disable an entry in the reference priority table. index = 0..15. state = 0 (disable), 1 (enable)
status	Displays information about the oscillator disciplining
syncstate	Display timing system synchronization state
sysupgrade	Performs system upgrade using the update bundle provided
testevent	Generates SNMP events in the enterprise MIB
tfomget	Displays current estimated system time error (TFOM – Time Figure of Merit)
timeget	Displays current system time (time is displayed in the configured timescale – See scaleget command to retrieve configured timescale)
timeset	Used to manually set the current time (hours, minutes in seconds); time is entered based on the configured timescale See scaleget command to retrieve the configured timescale
unrestrict	Used for clearing access control restrictions to VersaSync
version	Displays the installed main VersaSync and timing system software versions
yearget	Displays the current year
yearset	Used to set the current year
zeroize	Applicable to SAASM-equipped VersaSync units only

CTL linux commands (journalctl, systemctl)

C) What is Journalctl used for?

Journalctl is a utility for **querying and displaying logs from journald, systemd's logging service**. Since journald stores log data in a binary format instead of a plaintext format, journalctl is the standard way of reading log messages processed by journald.

To see the logs that the `journald` daemon has collected, use the **journalctl** command.

D) What is Systemctl used for?

The `systemctl` command **manages both system and service configurations, enabling administrators to manage the OS and control the status of services**. Further, `systemctl` is useful for troubleshooting and basic performance tuning.

<https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units>

Journal commands (screenshot below from VersaSync at v1.8.0)

```
spadmin@versaasync-0c0016:~$ journalctl
.bash_history .lesshst      cert/      cert.csr   config/    customize/ default/   log/       mibs/     update/   xfer/
spadmin@versaasync-0c0016:~$ journalctl
.bash_history .lesshst      cert/      cert.csr   config/    customize/ default/   log/       mibs/     update/   xfer/
spadmin@versaasync-0c0016:~$ journalctl
```

journalctl -fu ori

(screenshot below from v1.8.0, with Versa in Sync)

```
Sync Status: TIME
spadmin@versaasync-0c0016:~$ journalctl -fu ori
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Starting pptp1
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: All instances started!
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] Starting...
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] eth1 is in Master Only mode
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] Starting time transfer for eth1
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Started port state change routine
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Starting update routine
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] Waiting for all ports to be connected before running pptp1
Feb 27 21:55:06 versaasync-0c0016 ori[1359]: [eth0] eth0 is now LISTENING
Feb 27 21:55:12 versaasync-0c0016 ori[1359]: [eth0] eth0 is now MASTER
```

journalctl -u ori

(screenshot below from v1.8.0, with Versa in Sync)

```
spadmin@versaasync-0c0016:~$ journalctl -u ori
Feb 27 21:55:05 versaasync-0c0016 systemd[1]: Started Ori - the linuxsep manager daemon.
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: Starting enabled instances...
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: Starting eth0
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: Starting eth1
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Starting...
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] eth0 is in Master Only mode
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Starting time transfer for eth0
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] All ports connected
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Starting pptp1
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: All instances started!
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] Starting...
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] eth1 is in Master Only mode
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] Starting time transfer for eth1
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Started port state change routine
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth0] Starting update routine
Feb 27 21:55:05 versaasync-0c0016 ori[1359]: [eth1] Waiting for all ports to be connected before running pptp1
Feb 27 21:55:06 versaasync-0c0016 ori[1359]: [eth0] eth0 is now LISTENING
Feb 27 21:55:12 versaasync-0c0016 ori[1359]: [eth0] eth0 is now MASTER
```


systemctl status ori

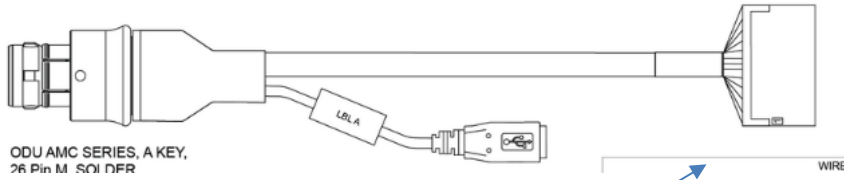
(screenshot below from v1.8.0, with Versa in Sync)

```
* ori.service - Ori - the linuxptp manager daemon
   Loaded: loaded (/usr/lib/systemd/system/ori.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-02-27 21:55:05 UTC; 15h ago
     Main PID: 1359 (ori)
        CPU: 22min 19.748s
     CGroup: /system.slice/ori.service
            └─ 1359 /usr/bin/ori
               └─ 1396 /usr/sbin/pmc -d 0 -t 0x0 -b 0 -us /var/run/ptp41-eth0
                  └─ 31107 /usr/sbin/pmc -d 0 -t 0x0 -u -b 0 -s /var/run/ptp41-eth0 "set total_time_inaccuracy_np internalTimeInaccuracy 1000000000"

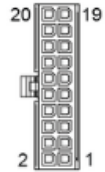
Feb 27 21:55:05 versasync-0c0016 ori[1359]: [eth0] Starting ptp41
Feb 27 21:55:05 versasync-0c0016 ori[1359]: All instances asserted!
Feb 27 21:55:05 versasync-0c0016 ori[1359]: [eth1] Starting...
Feb 27 21:55:05 versasync-0c0016 ori[1359]: [eth1] eth1 is in Master Only mode
Feb 27 21:55:05 versasync-0c0016 ori[1359]: [eth1] Starting time transfer for eth1
Feb 27 21:55:05 versasync-0c0016 ori[1359]: [eth0] Started post state change routine
Feb 27 21:55:05 versasync-0c0016 ori[1359]: [eth0] Starting update routine
Feb 27 21:55:05 versasync-0c0016 ori[1359]: [eth1] Waiting for all ports to be connected before running ptp41
Feb 27 21:55:06 versasync-0c0016 ori[1359]: [eth0] eth0 is now LISTENING
Feb 27 21:55:12 versasync-0c0016 ori[1359]: [eth0] eth0 is now MASTER
^
```

I/O Cable and I/O Breakout cable

- I/O breakout cable connects to the end of the I/O cable
- Breakout cables are not included with the purchase of base VersaSync. They are included with purchase of optional VersaSync Evaluation Kit (VEK).



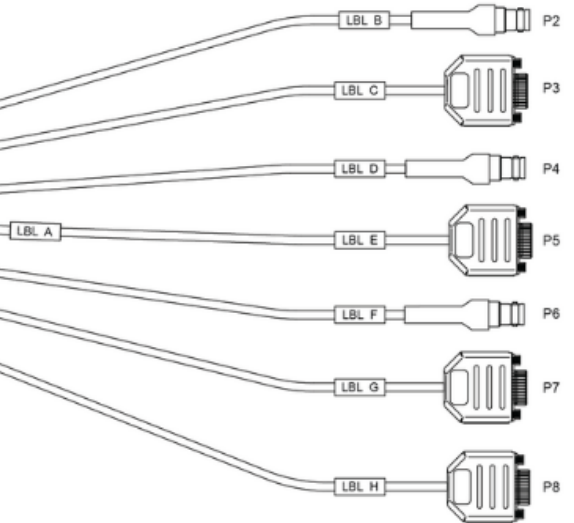
VIEW ON
FRONT VIEW



P1

WIRE DATA

WIRE ITEM No.	CUT			ROUTE FROM		ROUTE TO				
	PAIR	REFERENCE COLOR	AWG	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	
10	-	CONDUCTOR	26	12 IN	P1-1	12	9	P2-CTR	-	5
10	-	BRAID	-	12 IN	P1-2	12	9	P2-SHLD	-	5
11	1	RED	22	12 IN	P1-3	3	9	P3-1	-	7
11	-	BRAID	-	12 IN	P1-4	3	9	P3-5	-	7
11	1	BLACK	22	12 IN	P1-5	3	9	P3-2	-	7
-	-	-	-	12 IN	P1-6	-	9	-	-	-
10	-	CONDUCTOR	26	12 IN	P1-7	12	9	P4-CTR	-	5
10	-	BRAID	-	12 IN	P1-8	12	9	P4-SHLD	-	5
11	2	RED	22	12 IN	P1-9	3	9	P5-2	-	8
11	2	BLACK	22	12 IN	P1-10	3	9	P5-5	-	8
10	-	CONDUCTOR	26	12 IN	P1-11	12	9	P6-CTR	-	5
10	-	BRAID	-	12 IN	P1-12	12	9	P6-SHLD	-	5
11	3	RED	22	12 IN	P1-13	3	9	P7-2	-	7
11	3	BLACK	22	12 IN	P1-14	3	9	P7-5	-	7
11	4	RED	22	12 IN	P1-15	3	9	P8-1	-	8
11	-	BRAID	-	12 IN	P1-16	3	9	P8-5	-	8
11	4	BLACK	22	12 IN	P1-17	3	9	P8-2	-	8
-	-	-	-	-	P1-18	-	9	-	-	-
-	-	-	-	-	P1-19	-	9	-	-	-
-	-	-	-	-	P1-20	-	9	-	-	-



Certification of the breakout cables

Q Are the eval kit cables built by Orolia utilizing an aircraft certified classification so these can be used airborne (or are they round testing/reference only)?

A (per Ron Dries ~4 Apr 2019) The cables are not certified for aircraft. They are for lab integration.

**Options connector (Optional I/O connector)

- Used in conjunction with the Option Board (if installed)
- If Option Board is not installed, this connector is not used

**Options connector

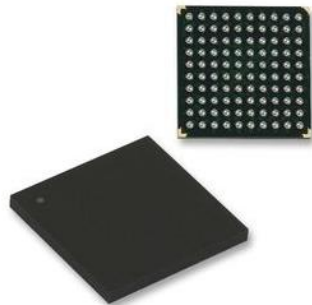
P240R-0081-002F: In Arena at: https://app.bom.com/items/detail-spec?item_id=1214648098&version_id=10607724118

Ref Des	Description	Spectracom part number	VersaSync Panel Connector	Mating connector (to be used for external cable)	Spectracom mating part number
J3	Option Connector, 8 pin	J240R-0081-012F	GK1YDR-P08UF00-000L	S11YDR-P08XFG0-0000	P240R-0081-002F

Q For the Power and Ethernet connector, what is the special tooling that is required?

A (per Ron Dries ~4 Apr 2019) https://www.odu-usa.com/fileadmin/redaktion/downloads/downloadcenter/assembly-instructions/ODU_AMC_Assembly_Instructions_Push-Pull.pdf

eMMC Flash memory – no Compact Flash (CF) card installed in VersaSync/VersaPNT



- VersaSyncs/VersaPNTS use **eMMC Flash** memory (Surface Mount component – Not a card)
 - These products don't use Compact Flash (CF) cards
- **Our P/N:** U060R-F8GB-000P
- Ref ID: U57
- **Description:** IC, SM (Surface Mount), eMMC MLC FLASH, 8GByte, 3.3V, LGA100, TBGA100
- Vendor part Numbers ISSI P/N [IS22ES08G-JQLA1](#)

(April 2019 Note) the VersaSync/VersaSync user guide incorrectly references “Compact Flash card” . Danny Loke pointed this out to Rachel:

Email from Danny Loke (April 2019) “VersaSync uses **eMMC Flash** memory, not Compact Flash card memory.”

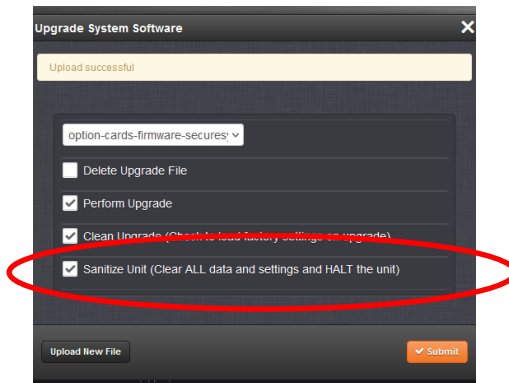
Sanitization/Certificate of Volatility (COV) / Letter of Volatility (LOV)

- “COV-VersaSync” in Arena at: https://app.bom.com/items/detail-spec?item_id=1277556469&version_id=11523411498
- “COV-VersaPNT” in Arena at: https://app.bom.com/items/detail-spec?item_id=1277550159&version_id=11523101358

(Versions 1.8.0 and above) Full Sanitization capability added to the Software Update functionality (as an available checkbox selection in the *Tools-> Upgrade/Backup* page)

Refer to the VersaSync online user guide at:

https://orolia.com/manuals/VSS/Content/NC_and_SS/2400/ADMIN/Sanitizing2.htm



Added in “customer-available” update version 1.8.0 (~Dec 2022). “Unofficially” added in 1.7.0, which was ultimately cancelled.

- Sanitization function not available in versions prior to 1.7.0 or below (1.6.0 was never released and 1.7.0 was cancelled. So, for customers, sanitization not available in versions 1.5.0 or below. Need to update to **1.8.0** or above to add it
- “Unofficially” added in the version 1.7.0 update (1.7.0 update was ultimately cancelled/changes rolled into 1.8.0).

Per the 1.7.0 Release Notes: “Added full Sanitization support in the Web UI and CLI. Sanitizing the unit will remove all user-related data, location history, usage statistics, etc., rewrite both partitions with clean software, and return the unit to a state completely without user data. Full status reporting of the sanitization process is available through the serial connection.

- It’s “officially” available in update versions 1.8.0 and above (~Dec 2022)

Note about updating from 1.5.0 to 1.8.0: v1.8.0 update file is a “.squashfs” file. Must first perform a “step update” to version 1.7.0 (v1.7.0 is a “.tar.gz” file). Then, version 1.8.0 can be applied to version 1.7.0.

Available Serial interface “feedback” during the sanitization process (excerpt below is from the user guide at same link above: https://orolia.com/manuals/VSS/Content/NC_and_SS/2400/ADMIN/Sanitizing2.htm)

Serial Feedback

The serial connection provides feedback during the sanitization process, even during states where the unit is otherwise unreachable, provides time estimates during each major state transition, and ends with the communication that the unit is being brought into a Halt state.

If you prefer, it is also possible to begin the sanitization process through the CLI. After uploading the desired file (via the Web UI, SSH, or some other desired connection), you can run the command `swupgrade [file] --sanitize`

Desire to physically remove eMMC Flash memory (U57) to sanitize Versa

- Refer to Salesforce Cases such as 263099
- eMMC memory is a Surface Mount component (U57) soldered to main PCB- not user removeable.
- There are no user-serviceable or user-removable parts in the Versas
- Removing memory would likely damage the Versa and void the warranty.

Email from Ron Dries (4 May 2021) As far as I know there are no user replaceable or removeable items in VersaSync.

The service team I believe already tells this to customers, if I remember correctly, I believe we say that customers need to send VersaSyncs back as nothing is field replaceable.

In a situation where they have a security requirement to physically remove the memory then I am guessing that would void the warranty and would be a lot of effort.

In the end I would believe it would be more practical to replace the unit.

My reply to customer (prior to sanitization being added via the version 1.8.0 update)

Regarding our Case Number 263099, thanks for your good (not strange) follow-up question!

This is going to sound strange, but I need to ask the question – The attached certificate of volatility provides a process to sanitize the non-volatile memory.

If the non-volatile memory had to be PHYSICALLY REMOVED due to a security issue, what would the level of effort be? Could this occur without de-soldering components or voiding a warranty? Would it be more practical to simply replace the unit?

My response

To begin, there are no user-serviceable, and no user-removable, components inside the VersaSync.

As shown below, the primary Flash memory (U57) is an IC soldered to the main PCB assembly. This component is not at all easily removed (just by desoldering it). It would need to be essentially "forced" off the PCB board, highly likely damaging the PCB and other nearby components. This action would definitely void the warranty!

*Inputs (Input References)/Sync-Holdover

Timing Interfaces (Standard Configuration)

Timing Inputs

GNSS L1, 72 Channel Receiver

- SMA connector, 5VDC to GNSS antenna

SAASM GPS, L1/L2 GPS (optional)

- Adds keyloader connection

DCLS Configurable Inputs (TTL level, 10V)

- 1 PPS
- IRIG B DCLS, HaveQuick

Time of Day Message (NMEA0183, HaveQuick)

- Over RS232, RS485

Network Inputs

- NTP Stratum 2
- IEEE1588 v2 slave

Number of available DCLS TTL outputs

Q Danny Loke asked me today about a VersaSync spec/configuration observation

He pointed out that page 2 of the VersaSync data sheet (under Timing Signals) shows the VersaSync can have a max of 2 inputs and a max of 5 outputs

Pulse/DCLS TTL level	1PPS, xPPS, IRIG, HaveQuick, alarm	Max: 2 inputs Max: 5 outputs
----------------------	------------------------------------	---------------------------------

Q But the Versa sync online guide, I/O connector pinout

table (<http://manuals.spectracom.com/VSS/Content/VSS/SETUP/Connecting.htm>) shows a total of **three** inputs (two pins for Have Quick RS-485 input, 1PPS input, and ASCII RS-232 input).

And this same table shows only **four** outputs (1PPS out 5V, 1PPS out 10V, ASCII out, and two pins for Have Quick RS-485 out) Why is there a difference between the data sheet and the I/O table.

A Reply from Ron Dries (6 Apr 2018) Please see the tool on this page of the VersaSync online manual: <http://manuals.spectracom.com/VSS/Content/VSS/SETUP/IOPinConfiguration.htm?Highlight=I/O> This shows that you can configure 5 TTL outputs and 2 TTL inputs.

Input references

**Chrony NTP Input Reference (NTP Peering/NTP server modes for “Stratum 2” sync)

NTP peering/NTP server mode

- Refer to Salesforce Cases such as 200269

The client *apparently* never loses NTP sync during these periods.

- NTP Peer/Server modes not “**operational**” in at least versions 1.3k and below
- Fixed in **VelaSync** v1.1.2 (~June 2019), but fix has not yet been ported into VersaSyncs, as of at least v1.3K
 - Per the VelaSync version 1.1.2 Release Notes “**Fixed an issue preventing Stratum 2 NTP operation without an active timing reference.**”

Per conversation with Denis R (2 July 2019): in previous VelaSync software versions 1.1.0 and 1.1.1, the TSync board inside the VelaSync was always being used by Chrony as a valid input reference (whether the TSync-PCIe board was synced to GPS, in Holdover mode, or if it was not in sync/not in Holdover). This was causing Chrony NTP in the VelaSync to always be a Stratum 1 time sever! It wouldn't switch to Stratum 16 upon loss of all valid input references.

Since GPS input to Chrony takes priority over NTP peers/NTP servers, TSync input always being considered by Chrony to be a valid input in versions 1.1.0 and 1.1.1, it would never switch to other NTP peers/servers as its selected reference (“TSync GPS is always valid, so why should I switch to an NTP input”).

Email from Denis Reilly (2 July 2019)

That release note refers to ticket SWI-619.

Velasync 1.1.1 and prior versions of software would use the embedded timing system as a source for NTP, no matter what its state was. So the Velasync would always show up as Stratum 1 NTP, and other NTP servers would never be used, even if the timing system was not in sync to any reference and not in holdover.

In 1.1.2, when NTP looks to the timing system as a source, it now takes its sync status into account. So, assuming other NTP sources are present and working, NTP will transition to Stratum 2 once the timing system loses all references and is out of holdover. It may take the NTP sub-system a minute or so to fully transition once the system leaves holdover.

Configuration of NTP Peers/Servers

Management -> **NTP Setup** page of the browser, gear icon in NTP

1. Press the “+” sign on the right.

**PTP Input Reference (PTP Slave mode)

- Not currently available, as of at least March, 2019 (at least all variants of v1.3.1 and below)
- PTP Master mode only, currently available

****ASCII input Reference (RS-485 and/or RS-232 input/Ascii Time Code)**

- ASCII Time Code is abbreviated in the browser as “ATC”.

Configuration

Interfaces -> *ASCII Reference* (ASCII Input 0)

Screenshot from v1.1.5

The screenshot displays a configuration panel for the ASCII Reference. It features several rows of settings, each with a label on the left and a control element on the right. The controls include dropdown menus and a numeric input field. At the bottom of the panel, there is a 'Status' button on the left and a 'Submit' button on the right.

Format Group	Auto
Format	Auto-Detect
Offset	0
Timescale	UTC
PPS Source	Message
Baud Rate	9600
Data Bits	8 data bits
Parity	Parity none
Stop Bits	1 Stop Bit

Status Submit

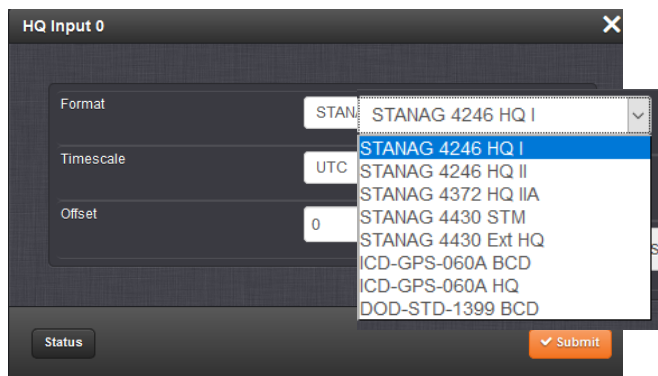
****HaveQuick Input Reference (HQ Input 0") into VersaSync**

Refer to online SecureSync user guide: http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_Stanag_In.htm

Configuration

Interfaces -> Havequick Reference (HQ Input 0)

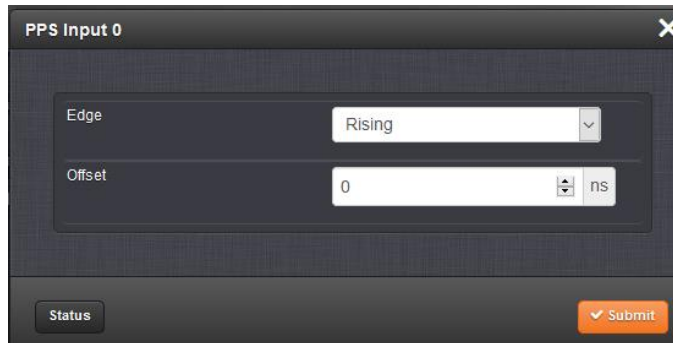
Screenshot from v1.1.5



****1PPS input Reference (“epp0”) into VersaSync
Configuration**

Interfaces -> PPS Reference (“PPS Input 0”)

Screenshot from v1.1.5



The screenshot shows a configuration window titled "PPS Input 0" with a close button (X) in the top right corner. The window contains two configuration fields: "Edge" is a dropdown menu currently set to "Rising", and "Offset" is a text input field containing "0" followed by a unit selector dropdown set to "ns". At the bottom left, there is a "Status" button, and at the bottom right, there is an orange "Submit" button with a checkmark icon.

*(J1) GNSS/GPS (uBlox receiver) and SAASM GPS



➤ SAASM-receiver capable

SAASM keyloader	DS101, DS102	Dedicated circular connector

Commercial GNSS antenna attached to connector J1



GPS/GNSS receiver is “receive-only” (it doesn’t transmit)

- For documentation indicating the GPS/GNSS receiver is “receive only”, refer to the “Model-specific” document: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\GPS\GPS is receive-only>

A) COMMERCIAL GNSS RECEIVER (ublox receiver)

- Refer also to “ublox Model M8T” receiver info in: <..\CustomerServiceAssistance.pdf>

GNSS Satellite Constellations

1. Galileo constellation

- VersaSync update version 1.1.5 added support for the Galileo constellation.

Receiver modes: Standard (Stationary) Mode/ Mobile mode/Mobile Position

- Refer to Online VersaSync user guide:
http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/CONFIG/GNSS_rec_mode.htm

1. Factory default mode: Mobile mode

- As of version 1.1.5 (Nov, 2017) The **default GNSS mode is now Mobile mode**, rather than Stationary. SW upgrades will not change the user-set configuration.

2. Standard (Stationary) mode/ GNSS survey

- As of version 1.1.5 (Nov, 2017) In Standard receiver mode and Stationary dynamics setting, on startup of the unit, a GNSS resurvey will now be performed automatically.

3. Manual position mode

- As of version 1.1.5 (Nov, 2017) The GNSS configuration now supports the Manual Position option which, in Standard receiver mode and Stationary dynamics, allows the user to manually set the geographic position. This may be necessary if the GNSS receiver could not complete a survey e.g., if GNSS reception is poor.

Max altitude with u-Blox M8T receiver

- Max altitude: per the VersaSync datasheet (under “**Environmental**” specs) is 45,000 ft

- Altitude: 45,000 ft

- Per the u-Blox M-8T datasheet https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_%28UBX-15025193%29.pdf

Operational limits ⁹	Dynamics	≤ 4 g
	Altitude	50,000 m
	Velocity	500 m/s

- Refer to Case 241304 for desire to exceed **45,000 ft** (for a high altitude balloon application)

3. Investigating if 45000 ft is for expected specs, or as high as the GNSS receiver will operate.

Email from Morgan Randolph (referencing Alex Payne with ODSI) 31 July 2020 The data sheet calls out 45k as the number, my question to Alex was did we have any data over the 45K spec.

B) SAASM GPS RECEIVER (Rockwell Collins MicroGRAM) and SAASM battery

SAASM receiver input is on “I/O (special)” connector



SAASM receiver information for Versas (status, operation, key loading, etc)

- Refer to the “VersaSAASMguide” (P/N: **1228-5000-0053**) along with other associated info in: <U:\Engineering\SAASM-FOUO\CustomerService\VersaSyncs>

Rockwells Collins MicroGRAM SAASM receiver

- **Our P/N for MicroGRAM:** MP30R-0GPS-0010 (in Arena): https://app.bom.com/items/detail-spec?item_id=1228754627&version_id=10719905748
- **Rockwell Collins P/N for MicroGRAM receiver:** 987-9705-012 (refer to sites such as https://www.rockwellcollins.com/~/_media/Files/Unsecure/Products/Product%20Brochures/Navigation%20and%20Guidance/GPS%20Devices/MicroGRAM%20data%20sheet.aspx)

M-Code (M Code) receiver/capabilities

- Contact OGSi Sales team (such as Trevor Dougherty)

Dept of Defense Form DD-1494 (DD1494 for SAASM)

- **Per Chris Shannon with Alion (18 feb 2021):** DD-1494 is “an entry into a Govt system to manage military transmitters and receivers. Pretty standard on the Govt side”

Refer to: "<I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8225S\DD-1494 Form>"

MicroGRAM Receiver major capabilities (not ITAR controlled and unclassified): per datasheet

<https://www.rockwellcollins.com/~media/Files/Unsecure/Products/Product%20Brochures/Navigation%20and%20Guidance/GPS%20Devices/MicroGRAM%20data%20sheet.aspx>

KEY FEATURES (SAASM)

- Capabilities of the Jaguar 12-channel GPS signal processor
- True All-In-View navigation of up to 12 GPS satellites
- Advanced correlator engine (ACE) turbocharges the engine for accelerated Direct-Y code acquisitions
- Next-generation security architecture provided by the key data processor (KDP 4)
- Unclassified-when-keyed operation
- Black key capable, for Over-The-Air-Rekeying (OTAR), when available from GPS satellites

MicroGRAM Receiver Specs (not ITAR controlled and unclassified): per datasheet:

<https://www.rockwellcollins.com/~media/Files/Unsecure/Products/Product%20Brochures/Navigation%20and%20Guidance/GPS%20Devices/MicroGRAM%20data%20sheet.aspx>

<p>KEY FEATURES (MICROGRAM)</p> <ul style="list-style-type: none">➤ Pick and Place compatible for ease of manufacturing➤ Same serial interface protocol as MPE-5➤ Selective Availability Anti-Spoofing Module (SAASM) security➤ 12-channel continuous satellite tracking for true All-In-View operation➤ L1 and L2 dual frequency GPS signal reception➤ Aggressive satellite acquisition/reacquisition strategies to improve performance and reduce power consumption➤ Cold start without time, position or satellite almanac in less than 110 seconds➤ Extended performance in a jamming environment<ul style="list-style-type: none">- 41 db while tracking- 24 db during initial satellite acquisition➤ User setup of units datums and coordinate formats➤ RTCM 194-93/SC 104 Differential GPS Correction Input➤ Mature, proven GPS technology <p>INTERFACE COMPATIBLE</p> <p>The MicroGRAM is an optimized lightweight, low power design that uses CMOS logic for efficient message protocol compatible with the MPE-5. The two low power serial data ports are full duplex interfaces with the MPE-5 heritage of ICD-GPS-153C. There are 1 pulse per second input and output timing pulses available for the host application to synchronize time. MicroGRAM provides DS-101 and DS-102 keying interfaces.</p> <p>DUAL FREQUENCY RF</p> <p>An advanced dual frequency RF front end allows track with both L1 and L2 GPS frequencies while minimizing the footprint on this miniaturized SAASM GPS receiver. Even when turned off, a precision time source runs continuously when auxiliary power is supplied to allow rapid acquisition of the GPS satellites when the MicroGRAM is turned on. Of course, all this capability requires only a single 3-volt power source.</p> <p>SPECIFICATIONS</p> <table border="0"><tr><td>System characteristics</td><td>Velocity: 1,200 m/sec maximum*</td></tr><tr><td>Dynamics</td><td>Acceleration: 9 g maximum</td></tr><tr><td>Time accuracy</td><td>100 nanoseconds</td></tr><tr><td>Position accuracy</td><td>DGPS: <2 meters CEP*</td></tr><tr><td>WAAS</td><td><4 meters CEP*</td></tr><tr><td>PPS</td><td><12 meters CEP*</td></tr><tr><td>Acquisition time</td><td>TTF (95%): <10 sec hot start, 90 sec warm start TSF (95%): <20 sec (E1 or S1b) <15 min TSF (95%): <55 sec (E1 or S1b) <60 min</td></tr><tr><td>Velocity accuracy</td><td>0.04 m/sec steady rate (SD 95%)</td></tr><tr><td>Coordinate system</td><td>8 redefined</td></tr></table>	System characteristics	Velocity: 1,200 m/sec maximum*	Dynamics	Acceleration: 9 g maximum	Time accuracy	100 nanoseconds	Position accuracy	DGPS: <2 meters CEP*	WAAS	<4 meters CEP*	PPS	<12 meters CEP*	Acquisition time	TTF (95%): <10 sec hot start, 90 sec warm start TSF (95%): <20 sec (E1 or S1b) <15 min TSF (95%): <55 sec (E1 or S1b) <60 min	Velocity accuracy	0.04 m/sec steady rate (SD 95%)	Coordinate system	8 redefined	<p>INTERFACES</p> <p>Interconnect</p> <p>RF connector Amphenol AMC RF Jack RA110</p> <p>Power and data Mini solder ball pins</p> <p>Hardware interfaces</p> <p>Two independent serial ports (full duplex CMOS)</p> <p>1 pulse per second input (CMOS)</p> <p>1 pulse per second output (CMOS)</p> <p>11,0/2 active RF antenna port, 3.3 V dc</p> <p>DS-101 and DS-102 key loading</p> <p>PHYSICAL CHARACTERISTICS</p> <p>Power</p> <p>Operating: 3.3 V dc, <0.5 W typical</p> <p>Sleep mode: 3.3 V dc, <0.3 mW typical</p> <p>Weight</p> <p>0.25 oz (7 gm) nominal</p> <p>Size/volume</p> <p>1.0" x 1.25" x 0.275" maximum</p> <p>[25.4 mm x 31.75 mm x 7 mm]</p> <p>Temperature range</p> <p>40° C to +85° C operating</p> <p>-55° C to +85° C storage</p> <p>Shock, all axes</p> <p>>600g, ½ sine, 1 msec.</p> <p>SPECIFICATIONS SUBJECT TO CHANGE WITHOUT NOTICE.</p> <p>* Export of precise positioning service (PPS) units is authorized for GPS Memorandum of Understanding countries only. PPS security modules must be obtained through foreign military sales (FMS) procurement.</p> <p>Building trust every day.</p> <p>Rockwell Collins delivers smart communication and aviation electronic solutions to customers worldwide. Backed by a global network of service and support, we stand committed to putting technology and practical innovation to work for you whenever and wherever you need us. In this way, working together, we build trust. Every day.</p> <p>For more information, contact:</p> <p>Rockwell Collins 400 Collins Road NE Cedar Rapids, Iowa 52498 +1.800.521.2223 +1.319.295.5100 fax: +1.319.378.1172</p>
System characteristics	Velocity: 1,200 m/sec maximum*																		
Dynamics	Acceleration: 9 g maximum																		
Time accuracy	100 nanoseconds																		
Position accuracy	DGPS: <2 meters CEP*																		
WAAS	<4 meters CEP*																		
PPS	<12 meters CEP*																		
Acquisition time	TTF (95%): <10 sec hot start, 90 sec warm start TSF (95%): <20 sec (E1 or S1b) <15 min TSF (95%): <55 sec (E1 or S1b) <60 min																		
Velocity accuracy	0.04 m/sec steady rate (SD 95%)																		
Coordinate system	8 redefined																		

Battery for SAASM receiver

- **As of at least (Aug 2019):** SAASM battery is not even mentioned in the SAASM user guide or the VersaSync user guide
- **excerpt of Email from Rachel (further below):** There is NOT an additional batter in SAASM units. Instead, the SAASM in a VersaSync connects to the BACKUP POWER in case of MAIN POWER failure, if the customer's power cables have anything hooked up to that. Otherwise, the SAASM just runs on the same power as the rest of the box.

Process Detail for a VersaSync/PNT with SAASM receiver (1228-XXXX-5000-PD) in Arena:

https://app.bom.com/items/detail-spec?item_id=1252489619&version_id=11325778298

Question Keith sent to Apps and others

Regarding VersaSync/PNT literature (such as the online user guide and the VersaSAASM guide 1228-5000-0053), Morgan just fielded a VersaSync customer call regarding if there is/are a battery/batteries in a SAASM option VersaSync, and if the batteries can be changed, etc.

Due to his call, I started looking to see exactly what info VersaSync/PNT customers are currently provided regarding any batteries installed (non-SAASM and SAASM). So, I simply searched for both "Battery" and "Batteries" in both the online user guide and the SAASM doc for Versas. With no hits on either word, I don't see where we may be currently providing any info to customers pertaining to batteries installed/need to be changed. I even looked at the SAASM PD and didn't see any reference to a battery.

All SecureSyncs have one Lithium battery for the RTC, and SAASM-equipped have a second battery.

- 1) Does this same info also apply to Versas? (is there a battery installed in all, a second installed for SAASM)?
- 2) If there is/are one or two Lithium batteries installed, are they customer-changeable, or require equipment return to the factory?
- 3) What is the recommended interval to change the battery/batteries?
- 4) Are there any externally provided indications of a battery needing to be replaced?

If this info is already battery available to customers, please let me know where it can be found (and my apologies for the email). If it's not already available to customers, can you please consider adding this info to the online user guide, SAASM guide, or even a separate document, if you prefer. Customers do periodically ask us for this type of info (as demonstrated by Morgan's call today). Having this info already available for customers (if it's not already) will be greatly appreciated by all 😊!!

Response from Rachel to Keith (2 Aug 2019 responding to my general questions about batteries in Versas)

Yes, there is a small RTC battery in a VersaSync. There is NOT an additional one in SAASM units. Instead, the SAASM in a VersaSync connects to the BACKUP POWER in case of MAIN POWER failure, if the customer's power cables have anything hooked up to that. Otherwise the SAASM just runs on the same power as the rest of the box.

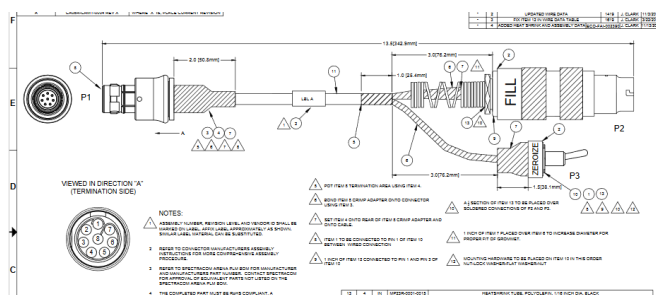
You're right, there currently really isn't any information about the VersaSync/PNT RTC batteries in the manual. The battery is a very tiny rechargeable Lithium battery that is directly soldered to the board itself. Since it is rechargeable and holding such a small amount of data, this battery is estimated to not fail or need to be changed at all during the lifetime of the product (I think maybe the worst case scenario is like 30 years based on our calculations). So there are no customer recommendations on that.

The only sign that the RTC battery had failed in a VersaSync/VersaPNT (and in the SecureSync 2400 as well) would be that the unit would no longer hold the time during shut down; there are no external indications.

I'll add a section clarifying this stuff into the next version of the manuals (it might take a while- I just renewed the revision!).

SAASM cable to SAASM connector (Keyfill and zeroize switch)

- Our P/N: CA08R-CRMT-0004 (in Arena at: https://app.bom.com/items/detail-spec?item_id=1241517384&version_id=11063976328)



Troubleshooting/known issues with SAASM GPS receivers

A) General troubleshooting info

Note: Always capture the **SAASM** receiver firmware and hardware version info (via a screenshot of the interface **INTERFACES > REFERENCES > SAASM GPS [x]**: Status window (“**Versions FOUO**” tab)

(12 Apr, 2019: not yet sure if all/part of this info is captured in the Manifest log)

B) Specific troubleshooting (carry-over from SecureSyncs- some or all may not pertain to VersaSyncs?)

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 SecureSync version 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 case 133596 (Aug, 2016 as reported by Ken Parks)
- 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)))

4. 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 Myers 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.

GPSD (a GPS service daemon) (applicable to versions 1.3.1 and above only)

- GPSD capability is currently only supported in VersaSyncs/VersaPNTs and 2400 SecureSyncs.
 - Standard feature available in firmware **versions 1.3.1** and above only
- Refer to online **VersaSync** user guide:
http://manuals.spectracom.com/VSS/Content/_Global/Topics/_GLOBAL/GPSD_Setup.htm?Highlight=gpsd
- Refer to online **VersaPNT** user guide:
http://manuals.spectracom.com/VSS/Content/_Global/Topics/_GLOBAL/GPSD_Setup.htm?Highlight=gpsd

Description GPSD is a free, open-source package used worldwide to manage GNSS systems and devices. With GPSD support on a VersaSync, users are able to:

1. Connect to the unit over a network via TCP at the specified port using any GPSD-compatible software
2. Receive position and timing information from the GNSS receiver in a consistent format, and
3. Use the WebUI (or CLI) to configure the GPSD service and view status information.

Per: <https://en.wikipedia.org/wiki/Gpsd>

gpsd is a daemon that receives data from a GPS receiver, and provides the data back to multiple applications such as Kismet or GPS navigation software. It thus provides a unified interface to receivers of different types, and allows concurrent access by multiple applications.

Design/port used

- gpsd uses **TCP port 2947**

gpsd provides a TCP/IP service by binding to port 2947.[4] It accepts commands from that socket, and returns results back to it. These commands use a JSON-based syntax and return JSON responses[4] (older, now obsolete versions used single-letter commands). Multiple clients can use gpsd's service in parallel, thus allowing multiple applications to use the data in parallel.

Most GPS receivers are supported, whether serial, USB, or Bluetooth. Starting in 2009, GPSD supports AIS receivers as well.[5] Additionally gpsd supports interfacing with the UNIX network time protocol daemon ntpd via shared memory to enable setting the host platform's time via the GPS clock.

(Year 2021) Date/Year rollover issue with gpsd (affects gpsd software versions < v3.23)

Summary: GPSD time will jump back 1024 weeks at after week=2180 (23-October-2021)

- Refer to sites such as: <https://gitlab.com/gpsd/gpsd/-/issues/144>
 - Refer to Salesforce Cases such as 270713 and 270805
 - Refer to JIRA Ticket CAR-1336
1. gpsd software update Fix (gpsd to v3.23) for 2400 SecureSyncs expected to be in v1.3.0 (around end of October 2021)
 2. gpsd software update Fix (gpsd to v3.23) for VersaSyncs expected to be in v1.5.0 (around end of Sept 2021)

Using GPSD with NTP/Chrony, to sync a Linux box

- Refer to sites such as (“GPSD TimeService HOWTO”): <https://gpsd.gitlab.io/gpsd/gpsd-time-service-howto.html>
 3. “GPSD, NTP and a GPS receiver supplying 1PPS (one pulse-per-second) output can be used to set up a high-quality NTP time server. This HOWTO explains the method and various options you have in setting it up.”

VersaSync/VersaPNT Requirements

1. I BELIEVE (not confirmed) Versa device MUST have commercially available uBlox receiver installed (not compatible with SAASM receiver)
 4. Refer to Salesforce Cases 185435/185456 (Feb 2019)
2. Installed VersaSync/VersaPNT software version needs to be **version 1.3.1 or above**

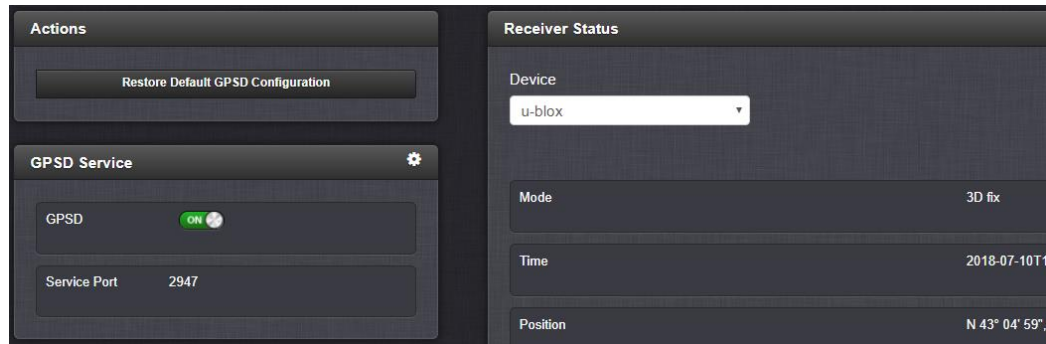
Per the version 1.3.1 update Release Notes: “Added GPSD support and GSPD configuration and display via VersaSync/VersaPNT CLI and WebUI. GPSD displays the status of the ublox receiver.”

GPSD Setup

- GPSD can only be configured to track the VersaSync internal u-blox receiver (GDPS does not currently apply to the internal IMU or gyro for navigation purposes).

A) GPSD via web browser

- To configure GPSD on the WebUI, navigate to **MANAGEMENT > NETWORK > GPSD Setup** to access the **GSPD Setup Screen**



The GPSD Setup Screen is divided into three panels:

4. The GPSD Service panel:

5. allows you to toggle the service ON or OFF
6. lists the Service Port
7. the **Gear** Icon in the GPSD Service panel allows you to change the Service Port information. If your GPSD setup changes and needs to be reconfigured within your VersaSync, this is where you can reset the service port.

5. The Actions panel

- provides an option to restore the default configuration.

6. The Receiver Status panel

- lists the information required by the GPSD service:

8. Device name
9. Mode, Time, Position, Track/Speed/Climb, Error Statistics, and Precision Statistics
10. All satellites in view and the PRN, Elevation, Azimuth, Signal Strength, and Usage for each satellite.

B) GPSD via CLI commands

The following CLI commands are used to control the behavior of Gpsd via the VersaSync CLI:

gpsdserviceportget – Displays the Gpsd service port

gpsdserviceportset – Sets the Gpsd service port

Gpsd utility programs

- There are two Gpsd utility programs already incorporated into VersaSync; GPSPipe and CGPS. Both can be used as commands within the CLI to view information currently being sent via Gpsd. Both commands use CTL + C to stop.

Navigational/motion (velocity) values obtained using gpsd

Velocity values

Error observed in velocity values (observed in 1.3.1G?)

- Refer to Salesforce Case 190878

Q When in stationary state the VersaSync is sending velocity values that are noise like (normal) that is in centimeters per second. However, it also gives a velocity error that is in fractions of millimeters per second instead in the range of centimeters per second (since the velocity is all noise).

A (reply from Keith, based on info from Ron Dries/Engineering (8 Apr 2019)) The engineers have confirmed there is a math error issue. A workaround for this issue is to scale the value we report by "6250", to get the correct value

Querying/Obtaining the current UTC offset from a VersaSync

- Refer to Salesforce Case 196859

Email from Ron Dries (31 May 2019) If they want to run a command on the VersaSync to pull the timescale offset they can use:

CS_GetTimeScaleOff 0 1

It will return:

Time Scale Offset for TAI: 37

The VersaSync will need a reference, GPS, that provides offset information for it to get the correct TAI offset.

DAGR/ICD-GPS-153C bi-directional interface

VersaSync vs DAGR

Q (from Viasat 6 Jan 2021) I am looking for a substitute for a DAGR to provide time and 1PPS (not position) to a MIDS JTRS radio in a test environment. This radio has an ICD-GPS-153C, bidirectional interface. Can the VersaSync, or another, simulate this interface? Based on the GSSIP section of the online user manual, it appears the VersaSync supports only 3 output messages and no receive messages or handshaking.

A reply from Tony DiFlorio (6 Jan 2021) Thank you for contacting Orolia. Is this the information in our VersaSync manual that you are referring to below? http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/APPENDIX/GSSIPMessForm.htm

Reply from customer Yes. The radio does the handshaking (ack/naks) with the DAGR per the '153 spec. Not clear whether the VersaSync can support this.

Reply from Tony Diflorio (11 Jan 2021) Here is the response from our team on your question; as I suspected, we do not support the bidirectional links.

"After reviewing, we don't have the bidirectional links necessary to the ASCII Output to support the handshaking on a standard VersaSync. It would require customization to try and support that capability. We can generate the GSSIP timing messages, but cannot simulate the message connection protocol without the bidirectional communication."

10 MHz Oscillator (OCXO) / CSAC MAC (Micro Atomic Clock), or Wentzel oscillator

- VelaSync is available with an installed 10MHz OCXO Oscillator, a CSAC or a MAC (Micro Atomic Clock)

Note: At least at this time, the MAC (Micro Atomic Clock) is a special option

A Reply from Tony D (15 MAR 16) better holdover than the CSAC (specified on the attached datasheet), we can offer a special option using the MAC (Micro Atomic Clock) instead of the CSAC. It consumes more power than the CSAC. The holdover for this MAC is better than the CSAC but needs to be investigated further to determine if it will meet this holdover spec.

Note: At least at this time, the Wentzel oscillator (for very low phase noise under shock/vibe conditions) is a special option.

OCXO oscillator

A) Y100R-0002-PH12

- Refer to (in Arena): https://app.bom.com/items/detail-spec?item_id=1203063005&version_id=10972419728&
- VCOCXO, TH, 10MHz, 5V, +/-10PPB, DIP9.5MM, -40C, 85C

Manufacturer: MAGIC XTAL LTD

MFG Part Number: MXO37/14P-F18C5S-10 MHz

Accuracy specs/Holdover / Holdover specs

Q Holdover must be less than 5uS over 5 days. Can VSync meet this holdover spec?

A Reply from Tony D (15 MAR 16) better holdover than the CSAC (specified on the attached datasheet), we can offer a special option using the MAC (Micro Atomic Clock) instead of the CSAC. It consumes more power than the CSAC. The holdover for this MAC is better than the CSAC but needs to be investigated further to determine if it will meet this holdover spec.

Time & Frequency Performances

Performances	OEXO	CSAC
Timebase Performances		
Relative Frequency Variation with Aging: - 24 hours - One month - One year	1.10 ⁹ 3.10 ⁸ 2.10 ⁷	- 3.10 ¹⁰ 1.10 ⁹
Relative Frequency Variation with Temperature (0°C to 60°C)	± 5.10 ⁸	± 5.10 ⁸
Short Term Stability (Allan Variance): @ 1 s @ 10 s @ 100 s	1.10 ⁹ 1.10 ¹⁰ 3.10 ¹¹	3.10 ¹⁰ 8.10 ¹¹ 3.10 ¹¹
Phase Noise on 10 MHz Output: @ 10 Hz @ 100 Hz @ 1 kHz @ 100 kHz	-110dBc/Hz -120dBc/Hz -140dBc/Hz -150dBc/Hz	-70dBc/Hz -113dBc/Hz -128dBc/Hz -140dBc/Hz
System Performances		
Frequency Accuracy Averaged Over 24 hour when Locked on GNSS	5.10 ¹²	1.10 ¹²
Phase (1 PPS) Drift in Holdover (no reference available) - 4 hours - 24 hours - 7 days	1.4 μs 45 μs 1 ms	0.2 μs 1.3 μs 30 μs
Phase (1 PPS) accuracy to UTC	±50 ns (1σ)	±50 ns (1σ)

discstats files

- 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 (
- 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)

11. **Seconds to xx:15=900**

12. **Seconds to xx:30=1800**

13. **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

14. **Sync and Holdover:** “1” is true, “0” is False

15. **DAC:** Believe this is the scaled DAC value for graph (not the actual DAC value)???

DAC value range for OCXOs is 00000 to max 65535

16. **Min D/A:** 0x0000 (00000 in decimal)

17. **Max D/A:** 0xFFFF (65535 in decimal)

18. **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 , $1 \times 10^{+/- 4}$, 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)

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,-1.44e-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
```

Software/Software updates/Software downgrade

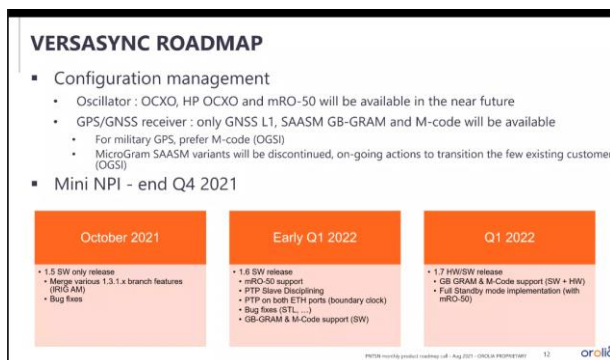
- Refer to online VersaSync user guide at:
http://manuals.spectracom.com/VSS/Content/VSS/SYSAD/SW_Upgrades.htm

Link to VersaSync software update bundles, update instructions and Release Notes:

<https://www.oroia.com/portal/public-downloads/latest-versasync-update-files/>

Link to spreadsheet of all VersaSync/VersaPNT version updates: <I:\Customer Service\PSB, PSP software updates\VersaSync and VersaPNT\VersaSync updates>

(Aug 2021) **do not distribute/internal use only**



- Software updates for units with commercial receivers are on our website (and are also in Arena)
- Updates for SAASM receivers need to be more controlled.

19. These updates aren't uploaded to our site – just available from Arena to send to a customer

SAASM receiver installed versus commercial/no receiver installed

per Jon Sinden (19 Dec 2018) Every VersaSync software update will include a SAASM version that we cannot put publicly on the website. You can get the SW off Agile and send it as a private link to a customer if needed.

Software update file Part Numbers

A) Commercial/no GNSS receiver installed

- P/N 1228-SU01-xxxx (where xxx is the version).
- In Arena at: https://app.bom.com/items/detail-spec?item_id=1227039810&version_id=10630169638&orb_msg_single_search_p=1

B) SAASM receiver installed

- P/N 1228-SU02-xxxx (where xxx is the version).
- In Arena at: https://app.bom.com/items/detail-spec?item_id=1227039810&version_id=10630169638&orb_msg_single_search_p=1

Software downgrades for fielded units

- Apparently, per Engineering, software downgrade is not possible with fielded units, in at least version 1.4.2 and below
- Customers who are locked-in at an earlier version and want to purchase newer units, need to specify their earlier version to be installed at the factory, before it ships. Otherwise, will need to be returned to factory for

Reset spadmin account password/password no longer known

- Refer to the VersaSync user guide at:
https://www.orolia.com/manuals/VSP/Content/NC_and_SS/Com/Topics/ADMIN/LostPassword.htm
 - Refer to JIRA ticket VPNT-789 (created 15 March 2023)
 - Need ability to locally reset spadmin password, or at least all configs via a method other than software login
- A) If the spadmin password is not known, but if another user-created account has been created (besides the spadmin account) and is known, spadmin account can be changed via the browser or reset via 'resetpw' cli command.
- B) If the spadmin password is not known, no other user-created accounts exist/are available, and if spfactory account still exists/remote login is allowed, can reset it via the spfactory account.
- C) As of at least March 2023 (and specific to JIRA VPNT-789) If the spadmin password not known, no other user-created accounts exist/are available, and the spfactory account has been removed/can't remote in, unit needs to be returned to factory.
- **Catch-22:** Can't sanitize it, without being able to first login!! Hence the reason for VPNT-789!

***Can bus interface (for vehicle information input)

- no info in yet in either online VersaSync/VersaPNT user guides (as of at least Nov 2019)
- Can bus (Controller Area Network)
- Looking at adding this interface in update version 1.04
- Refer to sites such as https://en.wikipedia.org/wiki/CAN_bus

A **Controller Area Network (CAN bus)** is a [vehicle bus](#) standard designed to allow [microcontrollers](#) and devices to communicate with each other in applications without a [host computer](#). It is a [message-based protocol](#), designed originally for [multiplex](#) electrical wiring within automobiles, but is also used in many other contexts.

***VICTORY interfaces (Vehicular Integration for C4ISR/EW Interoperability) for VersaPNTs

- **VersaPNT** is equipped with an interface that complies with the VICTORY (Vehicular Integration for C4ISR/EW Interoperability) standard. The use of the VICTORY interface is **optional**. Prior to using it, however, the interface needs to be configured.
- Refer to the online **VersaPNT user guide**:
http://manuals.spectracom.com/VSP/Content/VSP/VPNT_Vict.htm
- Refer to the VersaPNT "**Victory**" User Manual addendum (1228-5000-0054) in the **US ONLY** drive:
<U:\Documentation\Released\Manuals\1228-xxxx-xxxx\>

note this document is FOUO/ITAR controlled (Jon Sinden said this is particularly a US ARMY interface)

To determine if VICTORY is enabled in a VersaPNT (apparently not available with VersaSyncs)

1. Navigate to the **Management** tab in the web browser
2. If "**Victory Configuration**" is listed on the right-side of the Management drop-down, VICTORY is available/configurable)
 20. Refer to the VersaPNT "**Victory**" User Manual addendum (1228-5000-0054) in the **US ONLY** drive:

Network Related (eth0 and eth1)

**General Network Settings

- Refer to the online VersaSync user guide: <http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSSGenNWSettings.htm>

Network Ports (Interfaces eth0 and eth1)

- Refer to the online VersaSync user guide: http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_Netw_Ports.htm

Physical interface

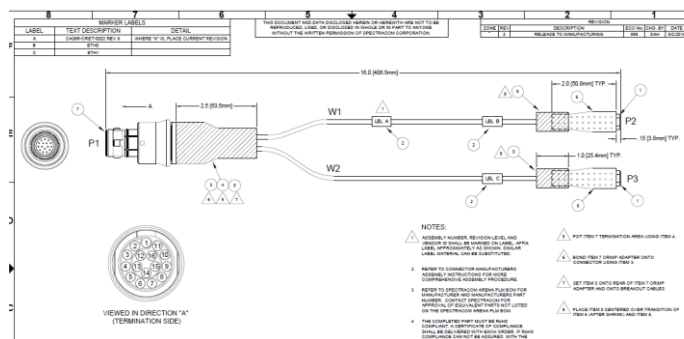
- Refer also to (in this same doc) “**Ethernet Interface (Ethernet) connector”
- VersaSync provides two different Gigabit Ethernet links (Eth0 and Eth1)



Interface	Type of Data	Connector
Ethernet in/out	NTP, PTP Navigation messages Monitoring	Circular

Ethernet breakout for eth0 and eth1

- For more info, refer also to (in this same doc) **Ethernet breakout cable (CA08R-CRET-0002) for eth0 and eth1
- Breakout cables are not included with the purchase of base VersaSync. They are included with purchase of optional VersaSync Evaluation Kit (VEK).
- Our P/N: **CA08R-CRET-0002** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1225621958&version_id=11339902938&orb_msg_single_search_p=1)



Factory default IP addresses for eth0 and eth1

Default IP addresses

ETH port	Default IP address
ETH0	192.168.1.1
ETH1	192.168.1.2

The default subnet is: 255.255.0.0

A) Assigning a Static IP Address Using the CLI:

Open the serial console, using a terminal emulator program

1. If necessary, disable DHCP – Command: **dhcp4set <x> off** (where x is 0/1 for ETH0 and ETH1, respectively).
2. Set the static IP address – Command: **ip4set <x>.<IP address>.<subnet mask>** Example: **ip4set 0 10.2.100.245 255.255.0.0**
If required, also set your gateway address: **gw4set <x> <gateway address>**
3. Verify that the address has been accepted – Command: **net4**
4. If so required, turn DHCP back on – Command: **dhcp4set [x] on**

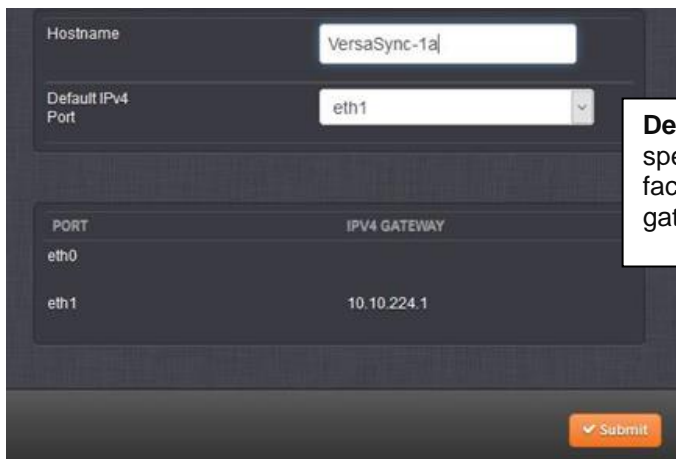
B) Via web browser

MANAGEMENT > Network Setup

**Main “Default IPv4 port” (main default IPv4 interface - main default IPv4 gateway)

- Refer to the online VersaSync user guide:
<http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSSGenNWSettings.htm>

Navigate to **MANAGEMENT** > **Network Setup**. In the Actions Panel on the left, click **General Settings**.



PORT	IPv4 GATEWAY
eth0	
eth1	10.10.224.1

Default IPv4 Port: Unless you specify a specific Port to be used as Default Port, the factory default port eth0 will be used as the gateway (default gateway).

Software Issue: Cant change “Default IPv4 Port” configuration.

(Applicable to at least versions 1.3.1K and below) There is an issue with not being able to change the main “default IPv4 port” to another interface (remains at the default port of “eth0”, even if you try changing it)

- Refer to Salesforce Case **208874** (Oct 2019)
- appears to be associated with JIRA ticket **SWI-674**
- “**Default IPv4 port**” defaults to “eth0”
- The browser field for selecting the main default interace ‘appears’ to be changing the value, but its not changing the associated file in the background (as observed via the CLI interface). So, the main default gateway interface is remaining as eth0.

Email from Jodi Campbell to her customer (31 Oct 2019) We tested this here as well. If we change the default IPv4 port under **Management>Network Setup>General Settings**, from eth1 to eth0, it is not reflected in PuTTY (SSH). Engineering has advised our Product Manager and is working with him on this. We will be opening a ticket.

Available work-around (per Pritam 14 Nov 2019)

They cannot change the default gateway port using the WEB-UI, in fact that function is not ported to Versa from SecureSync yet.

The work around for him is to go to command line and add a default route using Linux commands, something like this.

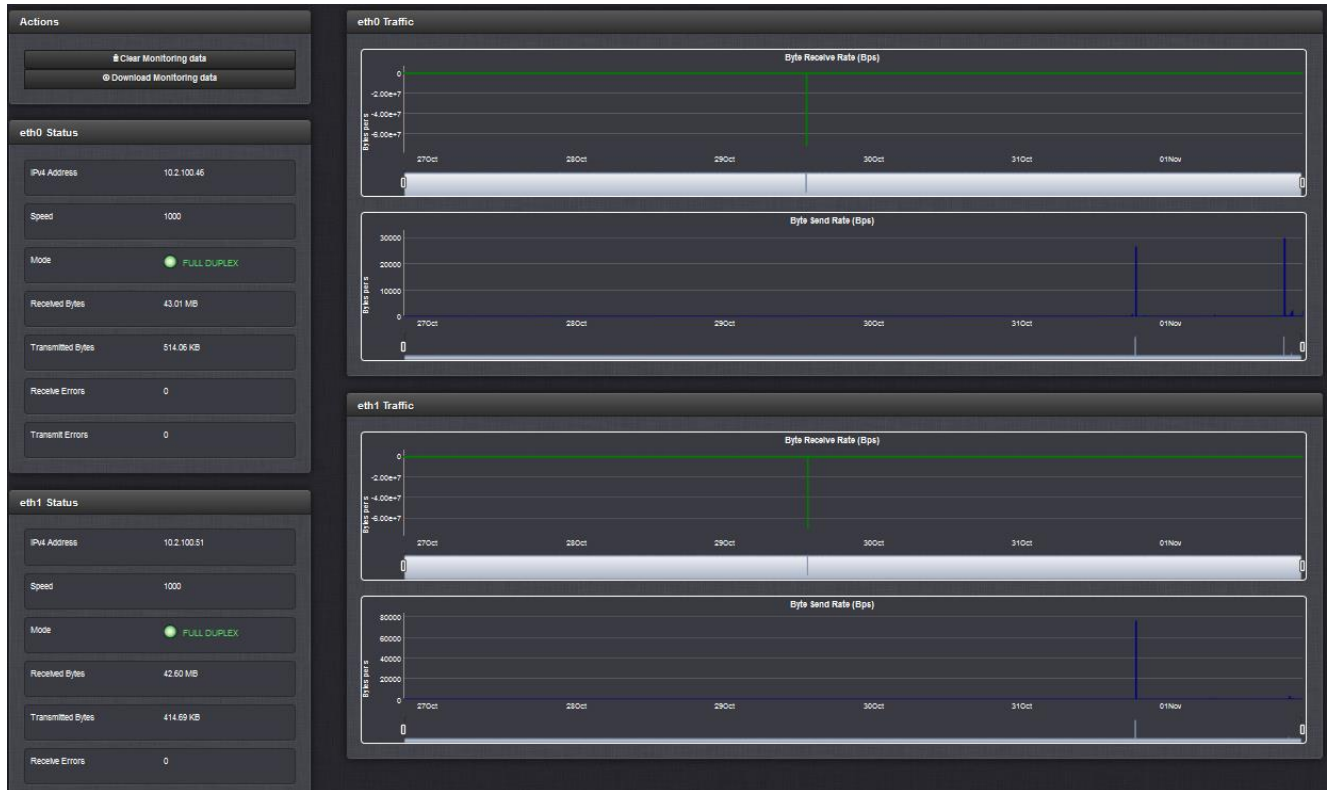
```
route add default gw 192.168.1.254 eth0 OR  
ip route add default via 192.168.1.254 dev eth0
```

Ethernet Monitor page and graphs

A) Eth0 and Eth1

Tools -> Ethernet Monitor page

- Refer to VersaSync user guide:
http://manuals.spectracom.com/VSP/Content/NC_and_SS/Com/Topics/OPRTN/Eth_Mon.htm
- Eth0 and eth1 transmit/receive graphs are in the **Tools -> Ethernet Monitor** page



B) Ethernet loading data for Eth0/Eth1

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

sys_timestamp	eth0_rx_bytes	eth0_tx_bytes	rx_bytes_per_s	tx_bytes_per_s	eth1_rx_bytes	eth1_tx_bytes	rx_byt
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
2017-07-12 2...	0	0	0	0	72067907	85269044	63
2017-07-12 2...	0	0	0	0	72073434	85271833	90

Network Services (telnet/ssh, FTP/SCP, HTTP/HTTPS, tcpdump)

- Refer to online VersaSync user guide:
http://manuals.spectracom.com/VSS/Content/VSS/SETUP/VSS_NetwServic.htm

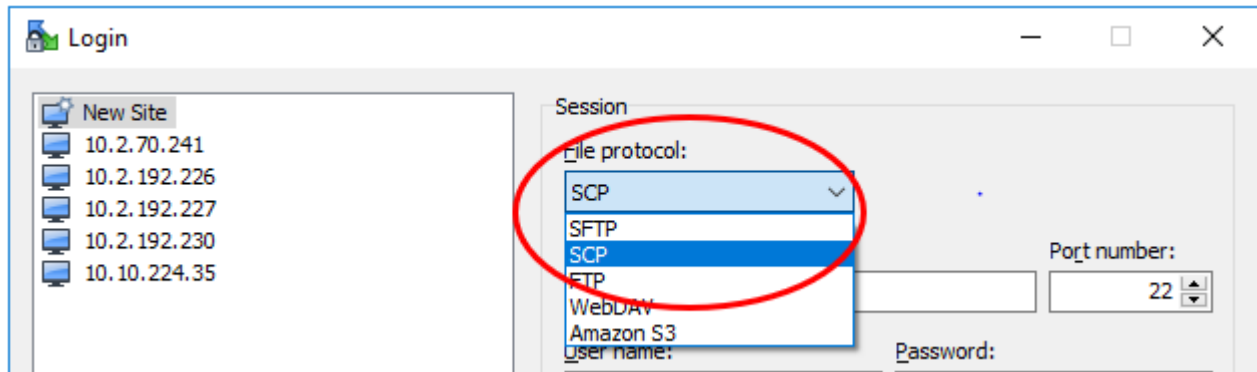
**SSH/SCP and FTP/SFTP, etc)

- Refer to online VersaSync user guide:
http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm

Note: I believe the below info about FTP/SCP is also correct for VersaSyncs (as it is for VelaSyncs)

FTP/SFTP are NOT currently supported (as of at least versions 1.3.1 and below)

- VersaSyncs only **support SSH/SCP**.
- They **don't support FTP/SFTP**
- **WinSCP** defaults to using "**SFTP**", so need to change/make sure its set to "**SCP**" for it to work with the VelaSyncs (as shown below):



Apache Web browser related

***User accounts/account names/passwords

- Refer to the online VersaSync user guide at:
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/UserAccounts.htm

Rules for Usernames

- **Length:** Usernames can be between 3 and 32 characters long.
- **Accepted characters:**
 - All letters, including the first, must be lower-case.
 - Numbers, underscores and dashes are accepted.
 - Next to punctuation symbols, the following special characters are NOT accepted: ! @ # \$ % ^ & * ()

Rules for Passwords

- The password requirements are configurable,
(http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/Passwords.htm)
- By default a password can be
 - any combination of upper- and lower-case characters.
 - Minimum password length = 8 characters,
 - maximum length = 32 characters

***Web UI TimeOut /web browser Idle login timeout (login time-out after no activity)

- Refer to online VersaSync user guide:
http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/OPRTN/Ultimeout.htm?Highlight=timeout
- Configured in “Minutes”
- Available timeout range is from **10 minutes to 1440 minutes (24 hours)**
 - factory default is **60 minutes**
- Click “**Web interface Settings**” on the left side of the *Management* -> *Network* page
- A change to the time-out period doesn't take effect until the NEXT login (not while already logged-in)



Web browser cache issue (need to periodically clean browser's cookies/cache)

- Refer to Salesforce Case 211355/JIRA tickets DMND-1076, DMND-1079
- Observed in 1.3.1C (but likely also present in at least 1.3.1K and below)
- Workaround "At this time, you are correct, to fix the problem, you'd just want to clean the cookies/cache of the web browser"

Customer Report: We encounter an issue with logging into the VersaSync unit and wanted to see if this is a bug or something we're doing wrong. We attempted to log in via the web UI and could not log in. We hook up a direct serial connection to the unit and was able to log in using the default credential but the same credential does not work on the web UI. We attempted to reset configuration using "clean" but the same issue persist. We also attempted to run "resetpw" on the cli but it reported the following:

```
=====  
>resetpw  
.conf file not present  
Error while reading .conf file!!!  
Error: LDAP Read Config  
=====
```

Do you know what we can do to log in to the Web UI again? For reference, we are running 1.3.1c.

Reply from Jodi (29 Jan 2020) This was reviewed with Engineering and it may be related to a known issue we are working to resolve. We have been able to duplicate it in our testing. We see the fix and are working to integrate it into the product.

At this time, you are correct, to fix the problem, you'd just want to clean the cookies/cache of the web browser.

****REST API interface/Postman (alternate to using the standard web browser or CLI)

- Here is a link to what we have for the REST API documentation in SecureSync:
<https://files.spectracom.com/client-downloads/5820>
- Refer also to documents (such as API guide) in: [\\rocfnp02\drive\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts\](#)
- allows for status and configuration data to be sent and retrieved without having to use the Web UI.
- uses the JSON data format when performing HTTP GET and POST operations

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://files.spectracom.com/client-downloads/5690>

Note this function requires **software versions 5.4.5** and above be installed.

In summary: the REST API allows anything available via the browser to be scripted, using programs such as python.

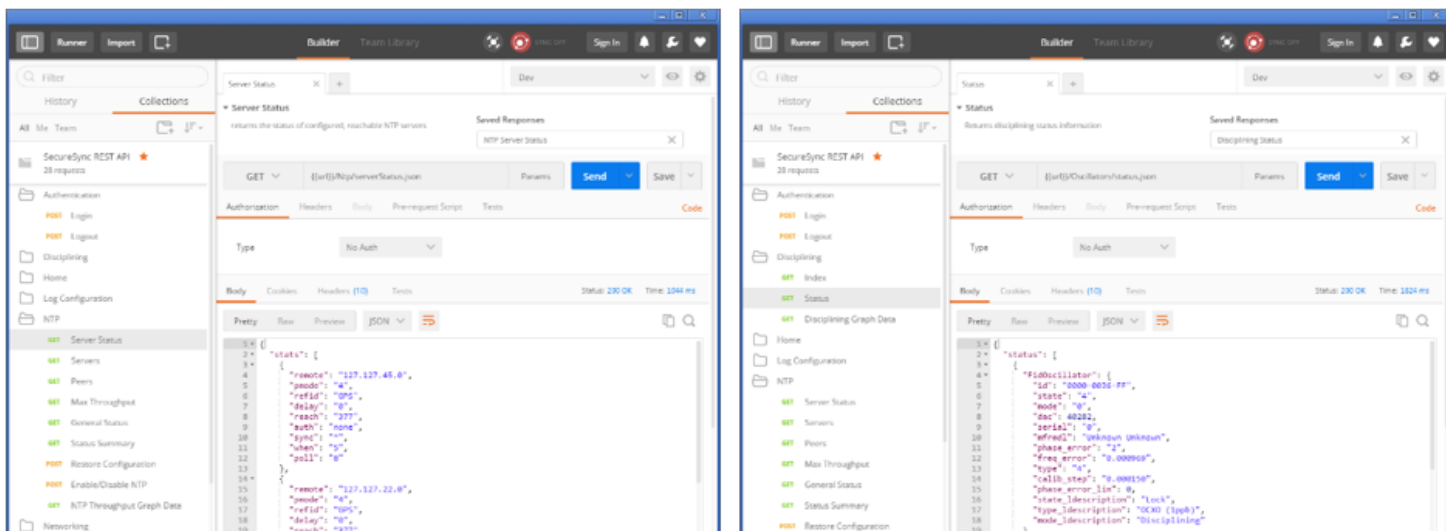
The graphical Web User Interface ("Web UI") used with Spectracom's SecureSync and 9400 series NetClock time servers have a built-in REST API which allows for status and configuration data to be sent and retrieved from the device without having to use the Web UI. This is useful for machine-to-machine 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™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.

OROLIA PROPRIETARY – COMPETITION SENSITIVE

REST API

Documented/Delivered as Postman Collection



Nagios®

Current Network Status
 Last Updated: Tue Jan 26 09:50:52 EST 2016
 Updated every 90 seconds
 Nagios® Core™ 4.1.1 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals
 Up: 1, Down: 0, Unreachable: 0, Pending: 0
 All Problems: 0, All Types: 1

Service Status Totals
 Ok: 8, Warning: 1, Unknown: 0, Critical: 0, Pending: 0
 All Problems: 1, All Types: 9

Service Status Details For Host 'eng-0016'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
eng-0016	CPU	OK	01-26-2016 09:44:55	49d 17h 4m 31s	1/3	1 CPU, load 70.0% < 85% : OK
	DISK	OK	01-26-2016 09:44:35	49d 17h 5m 2s	1/3	/: 42%used(401MB/946MB) (<70%) : OK
	ETH	OK	01-26-2016 09:48:11	4d 0h 32m 30s	1/3	eth0:UP (0.7KBps/0.6KBps):1 UP: OK
	GNSS	WARNING	01-26-2016 09:41:55	4d 0h 45m 7s	3/3	GNSS Warning, Antenna Open - 15 satellites tracked
	HTTPS	OK	01-26-2016 09:45:55	49d 17h 13m 11s	1/4	HTTP/1.1 200 OK
	MEM	OK	01-26-2016 09:46:06	49d 17h 3m 40s	1/3	Ram : 33%, Swap : 0% : OK
	NTP	OK	01-26-2016 09:46:55	49d 17h 13m 30s	1/4	NTP OK: Offset 1.6459001 secs
	PING	OK	01-26-2016 09:49:55	49d 17h 11m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.25 ms
	SSH	OK	01-26-2016 09:49:45	49d 17h 13m 13s	1/4	SSH OK - OpenSSH_6.9p1-hpn14v5 (protocol 2.0)

Results 1 - 9 of 9 Matching Services

Availability/support of the REST API

- 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.~~

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™** 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

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**)

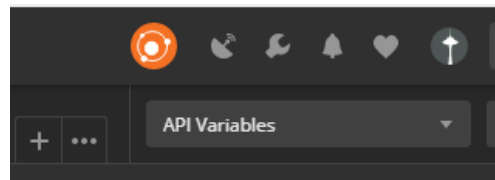
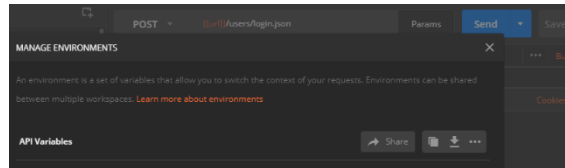
"To run the script, issue at the Windows command prompt the following command on a PC that has python installed (<https://www.python.org/downloads/release/python-352/>).

```
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 spadmin -p admin123
```

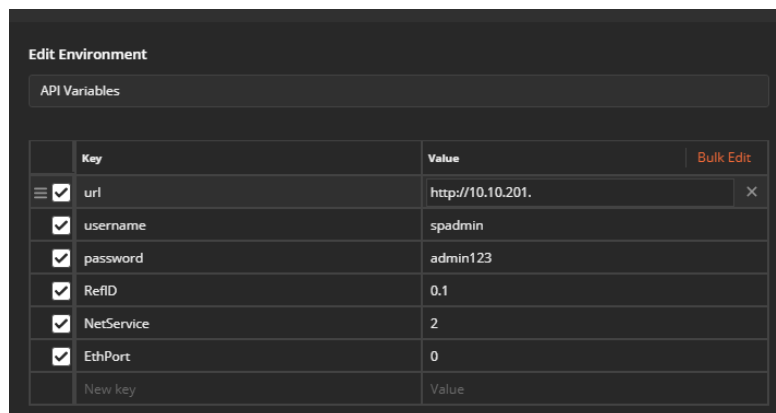
Postman details

- 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).

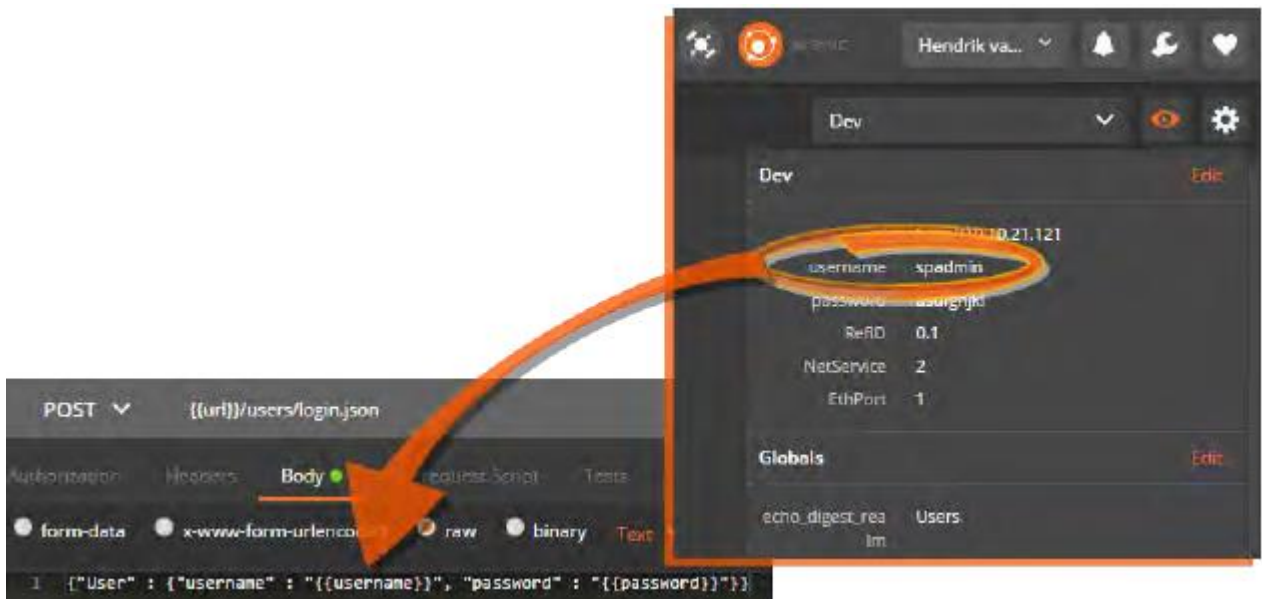


1. In the Environment drop-down menu (next to the EYE button), select Dev to load the environment imported above.
2. Click the **EYE** button to see which environment variables have been loaded with this environment file: One variable is called **url**, another one is **spadmin**, etc.

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:

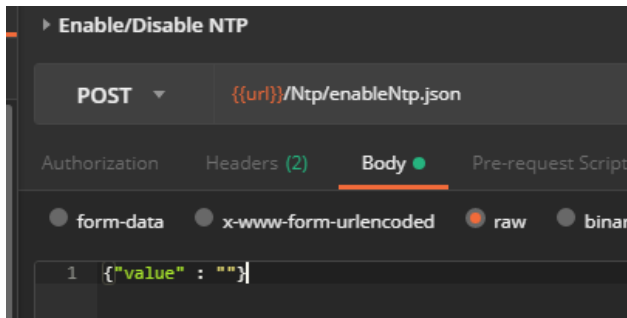


Login to the time server.

On the left-side of the page expand “SecureSync REST API”, expand and perform **Authentication** -> “**login**” to the desired SecureSync

- scroll down about 53 lines and verify it indicates (in white text) “**Welcome, spadmin**”
- this confirms you are logged into the time server. No need to login again for each task desired to be performed

For “**Get**” commands (cannot edit Get commands), select the “**Body**” tab in the second main window down
 For “**Post**” commands (which allows edits of the values) select the “**Body**” tab and select “**JSON**” in the drop-down.
 then select “**raw**” on the upper window to edit values (in yellow text).



Logout of the time server when done

On the left-side of the page expand “SecureSync REST API”, expand and perform **Authentication** -> “Logout” to the desired SecureSync

- scroll down about 53 lines and verify it indicates –(in white text)–

Specific examples where REST API can be used

- refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts\Python scripts](#)

A) 10 MHZ and 1PPS outputs

- Refer to Salesforce case 25034

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.**

B) download GPS status info

“Here is a simple python script (without error checking) to login and extract the GPS information and put it in a csv file.”

Apparent Issues associated with REST API

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™, or as native apps for Microsoft Windows™, 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.

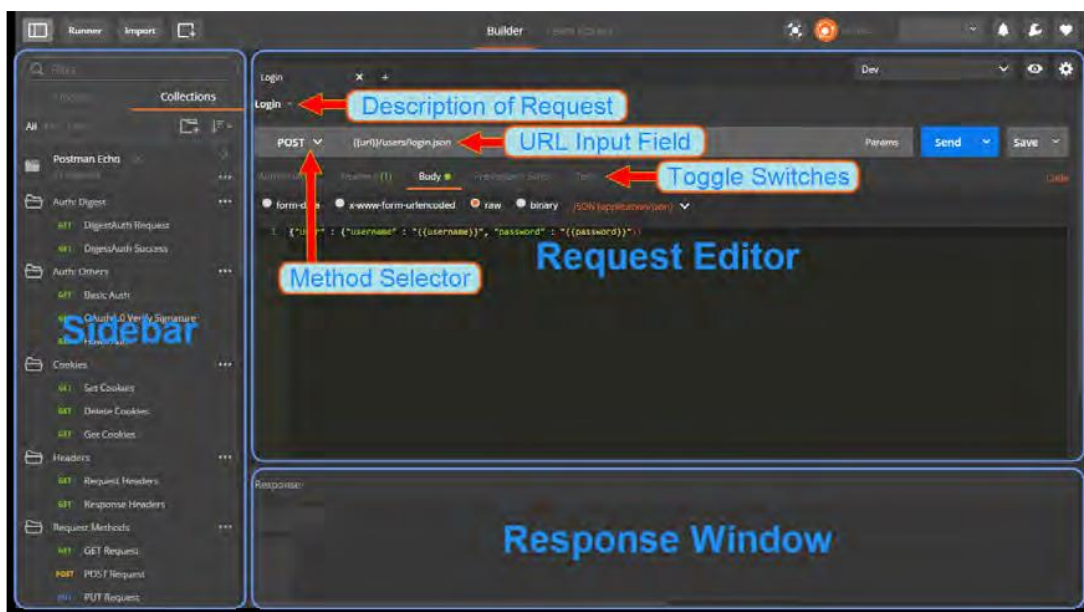
Downloading and Installing the Postman™ Chrome™ App

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

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.

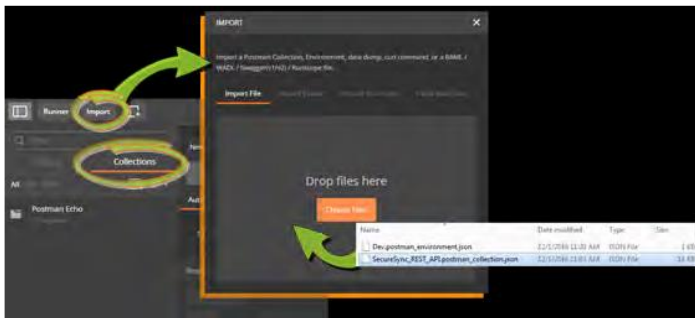
- Display responses in different formats e.g., "pretty", "raw", or as rendered HTML pages.
- Organize and store requests in Collections.
- Store request parameters that will be used repeatedly (e.g., keys and values used as login credentials) in development project-specific Environments.
- Access history 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.
 - a. Navigate to Collections > Import: Choose File.



- c. From the zip folder created in step 2, select the file `SecureSync_REST_API.postman_collection.json`, and open it. Under the Collections tab in the Sidebar on the left, SecureSync REST API will be displayed. Click on it to display the Collection's folders which reflects the menu structure of the SecureSync Web UI e.g., Networking, Log Configuration, NTP, etc. Each folder contains requests.

Click on any request to display it in the Request Editor.

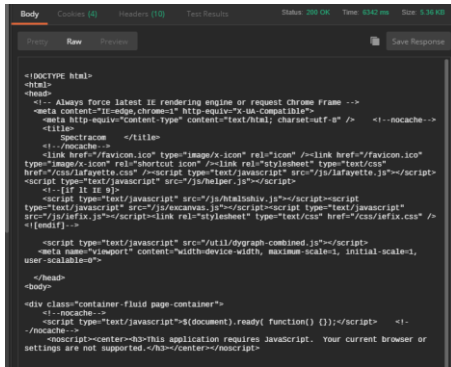
Importing the DEV Environment

The Development Environment includes a selection of variables/parameters that are frequently used when interacting with a SecureSync unit via the API.

To import the Development Environment:

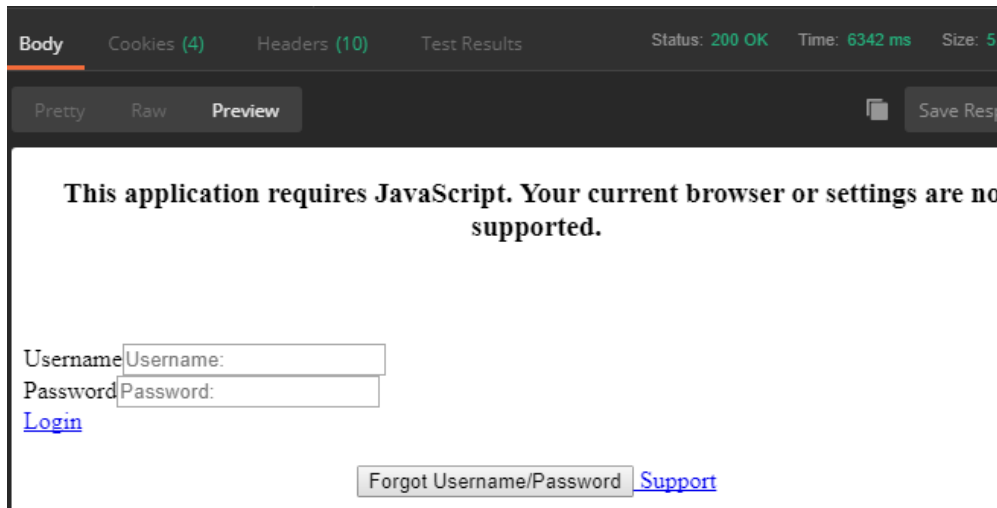
1. In Postman, click the GEAR button on the right, and select Manage Environments.
2. Click Import, navigate to the folder in which you unzipped the Spectracom API

Raw tab



```
<!DOCTYPE html>
<html>
  <!-- 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>
    Spectram
  </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/themer.js"></script>
  <!--[if IE 8]>
  <script type="text/javascript" src="/js/htabsdiv.js"></script><script
  type="text/javascript" src="/js/scanvas.js"></script><script type="text/javascript"
  src="/js/afix.js"></script><link rel="stylesheet" type="text/css" href="/css/afix.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-->
  <noscript><center><h3>this application requires javascript. Your current browser or
  settings are not supported.</h3></center></noscript>
</body>
```

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

Management Menu pages

screenshot *from VersaSync v1.3.1K (Oct 2019)*



****Management -> Time Management page / Local Clocks**

****System Time/Year and System timescale**

Newer browser: Management -> Time Management page of the browser

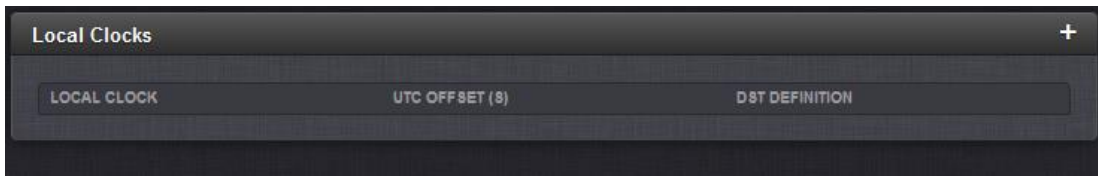


System Year / “Set Year Only” checkbox/field

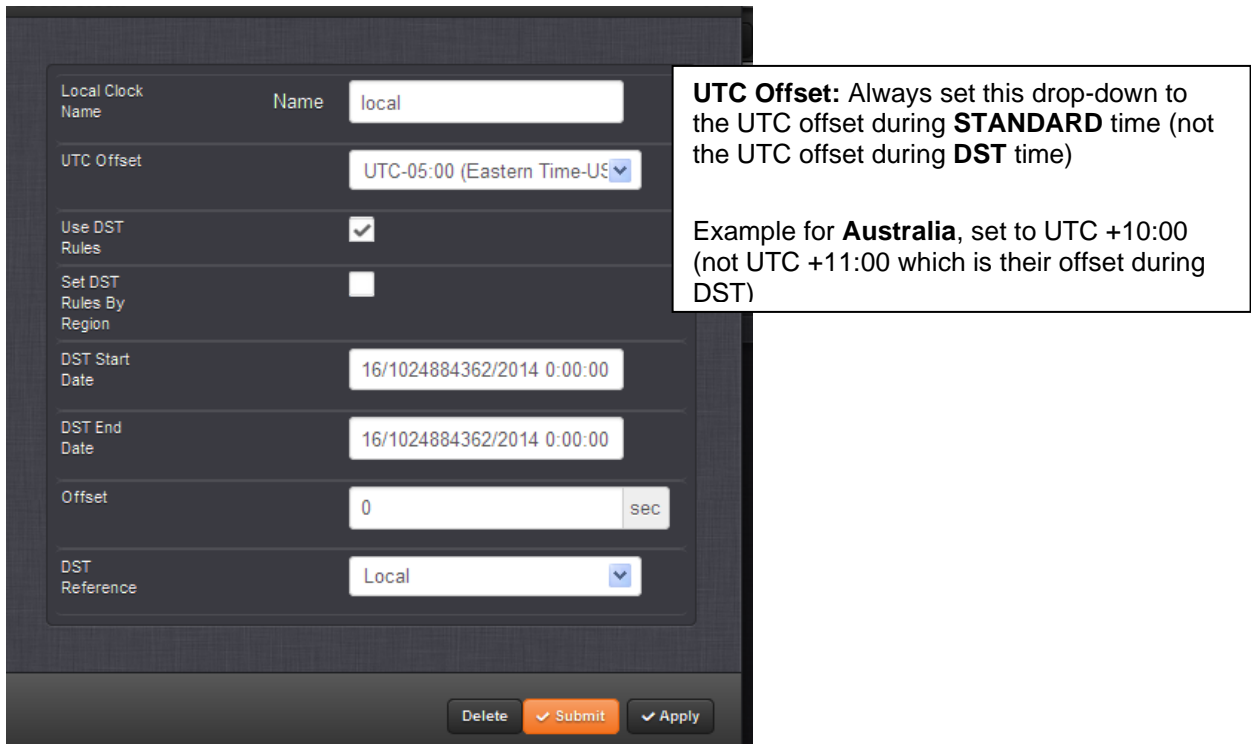
- With the exception of IRIG input having no year (such as B000), the year is normally set by the input reference.
- “Set year only” Checkbox/field is used when IRIG input doesn’t contain Year

**Local System Clocks (Local Clock)

Management -> Time Management (click on the + to add a new local clock)



If "Use DST rules" is selected, bottom of page expands.



The screenshot shows the configuration form for a local clock. The fields are:

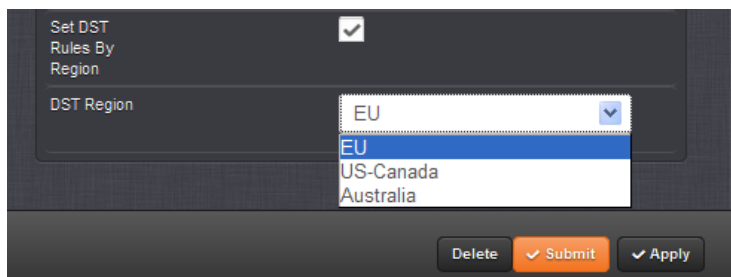
- Local Clock Name: local
- UTC Offset: UTC-05:00 (Eastern Time-US)
- Use DST Rules:
- Set DST Rules By Region:
- DST Start Date: 16/1024884362/2014 0:00:00
- DST End Date: 16/1024884362/2014 0:00:00
- Offset: 0 sec
- DST Reference: Local

Buttons at the bottom: Delete, Submit, Apply.

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.



The screenshot shows the configuration form for "Set DST Rules by Region". The "Set DST Rules By Region" checkbox is checked. The "DST Region" dropdown menu is open, showing the following options: EU, US-Canada, and Australia. Buttons at the bottom: Delete, Submit, 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 3600spadmin@Spe
```

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 Donal 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 of 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.

****System Time Message daemon (STMD)**

Management -> System Time Message page of browser

- Refer to “System Time Message” in SecureSync tech note: <..\SecureSync CustAssist.pdf>

Software issue with STMD (applicable to at least versions 1.3.1k and below): cant disable STMD daemon/service and associated packets on port 1024

- Refer to Salesforce case 219158
- **Refer to JIRA ticket”** VPNT-509 (hotpatch to disable STMD service)

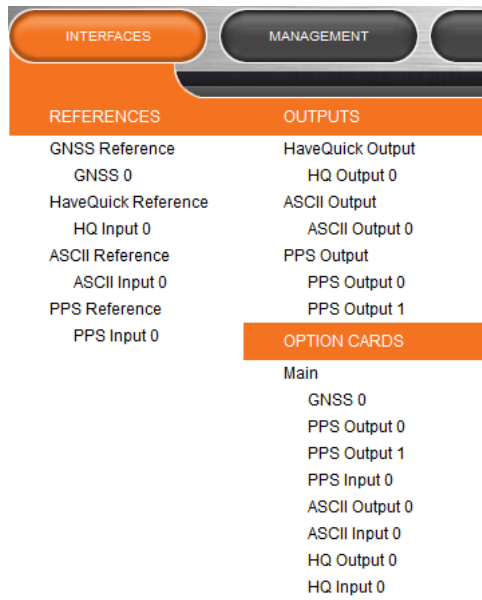
Email from Ron Dries (3 Jan 2020) The VersaSync I setup here was also seeing RRCP traffic similar to what the customer reported. The RRCP traffic is not originating from the VersaSync, the MAC address that is shown (50:d4:f7:14:4b:58) is not a VersaSync MAC address. I saved the output of tcpdump from the VersaSync and opened it in Wireshark and confirmed that the RRCP traffic was coming from one of our Netgear routers.

```
10:37:23.005885 IP versasync-0c01b7.1024 > 239.0.0.1.1024: UDP, length 20
10:37:23.894255 50:d4:f7:14:4b:58 (oui Unknown) > Broadcast, RRCP-0x25 query
10:37:24.005891 IP versasync-0c01b7.1024 > 239.0.0.1.1024: UDP, length 20
10:37:24.892775 ARP, Request who-has 192.168.1.1 tell 192.168.1.51, length 46
10:37:24.898455 50:d4:f7:14:4b:58 (oui Unknown) > Broadcast, RRCP-0x25 query
10:37:25.005915 IP versasync-0c01b7.1024 > 239.0.0.1.1024: UDP, length 20
10:37:25.895935 50:d4:f7:14:4b:58 (oui Unknown) > Broadcast, RRCP-0x25 query
10:37:26.006155 IP versasync-0c01b7.1024 > 239.0.0.1.1024: UDP, length 20
10:37:26.896279 50:d4:f7:14:4b:58 (oui Unknown) > Broadcast, RRCP-0x25 query
10:37:27.005913 IP versasync-0c01b7.1024 > 239.0.0.1.1024: UDP, length 20
10:37:27.897185 50:d4:f7:14:4b:58 (oui Unknown) > Broadcast, RRCP-0x25 query
```

However the highlighted traffic that is on port 1024 in the snippet I copied above from the customer is coming from the VersaSync. This is traffic from the System Time Message feature. The issue is that when this feature was ported to VersaSync the mechanism to stop this service was not ported. A JIRA ticket has been created to add this mechanism in a future software release. I spoke with Engineering this morning and we can have a software patch which disables the System Time Message feature early next week. This way the customer can stop that traffic now.

Interfaces Menu

screenshot *from VersaSync v1.3.1K (Oct 2019)*



Logs/Syslog

- Refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\Prisma Velasync\Alarms and logs](#)
- And in the Prisma Velasync online manual:
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 Prisma Velasync Logs are stored in the home/spectracom/log directory.

A) Syslog (Remote logs/remote logging)

- **Example freeware Syslog server software:**
 1. “Event Log Analyzer” <https://www.manageengine.com/products/eventlog/download-free.html>
 2. “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”
3. Refer to <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Prisma Velasync\Syslog>

RFCs for Syslog protocol

- Our syslog operation follows RFCs 3164 (obsolete) and 5424 (<https://tools.ietf.org/html/rfc5424>)
http://www.rfc-editor.org/search/rfc_search_detail.php?rfc=3164&pubstatus%5B%5D=Any

Syslog Protocol

- 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 messages/ UDP port number

SSL Encryption of logs being sent to Syslog servers

- As of at least versions 5.3.2 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:
 4. “**Local Logging**”: You can individually configure which log files get saved in the box (**Management** -> **Logs** page, in each log tab).
 5. “**Remote Logging**”: You can individually configure which log files get sent to Syslog (**Management** -> **Logs** page, in each log tab)

Prisma Velasync sends Syslog messages as UDP on port 514

UDP/Port Number

- Uses UDP port 514

Q Can syslog send logs via TCP instead of UDP

A Syslog sends logs via UDP port 514. Syslog in the Prisma Velasync isn't able to send logs via TCP.

FYI Syslog in the Prisma Velasync 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."

"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 Versa sent a log entry

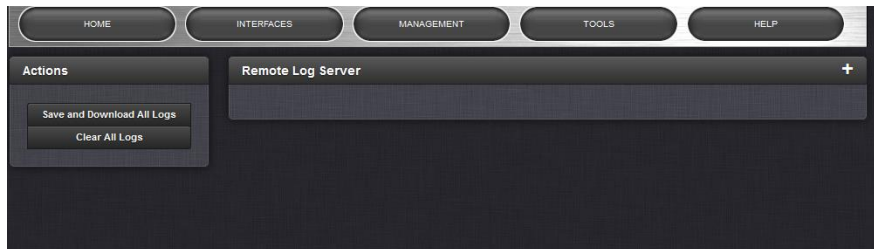
- Each log entries contain the DNS Hostname of the Versa

Configuration of syslog

** *Management* -> *Log Configuration* (syslog and download logs)

Remote Log server

- Refer to "Syslog" in SecureSync tech note: <..\SecureSync CustAssist.pdf>
screenshot from v1.1.0 (Nov 2018)



- Refer to syslog tech notes for Prisma Velasync

6. **Prisma Velasync** : <!:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Prisma Velasync\Syslog>

7. **9400 series**: <!:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\Syslog>

browser:

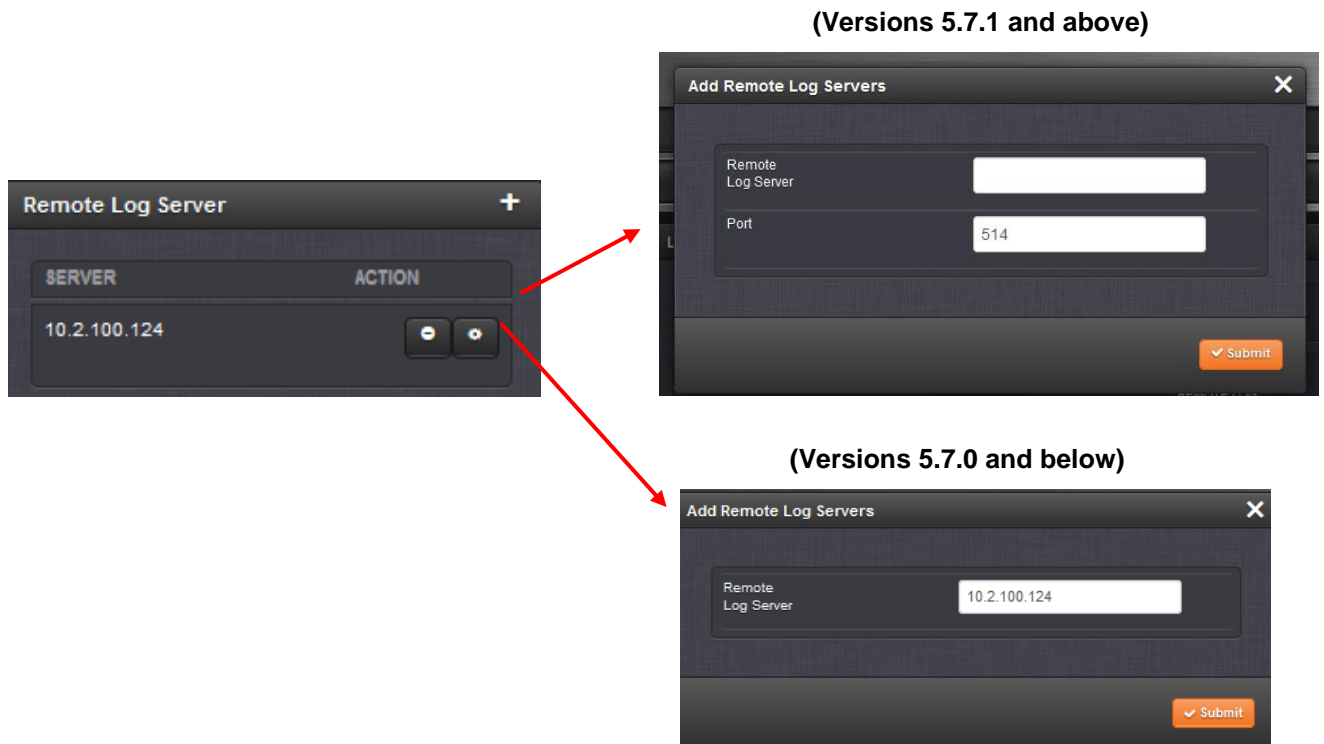
- Configured in each log of the *Management* -> *Log Configuration* page of the browser

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)



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

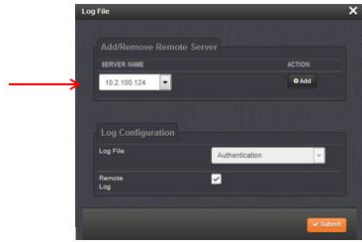
NOTE: due to ability to individually configure each log type to be able to be sent to different log servers, the user MUST individually “add” the syslog server for each log type.

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

8. Update version 5.7.1 (starting 6 Sept 17) and above now provide ability to delete just the syslog configuration.

9. 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

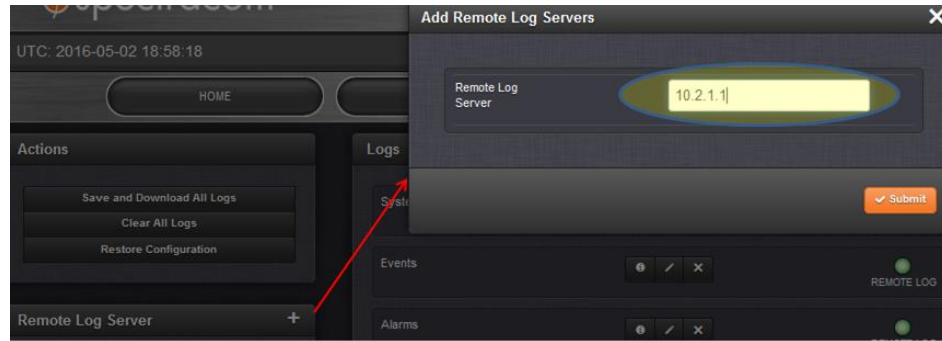
Email from Keith on how to configure syslog

All 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



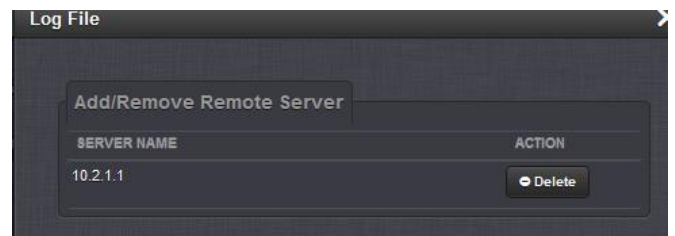
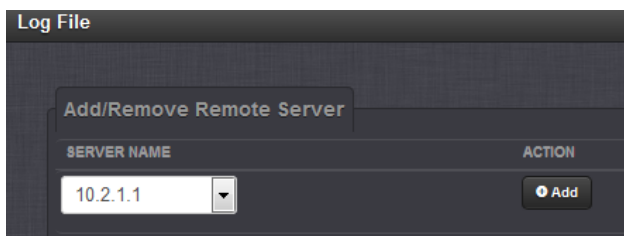
Because the log files can be individually configured as to which remote server its entries are sent to, each log file type (such as the System Log for example) has to be individually configured to be sent to the desired remote server, before its logs will be sent to any remote server. You need to add (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.

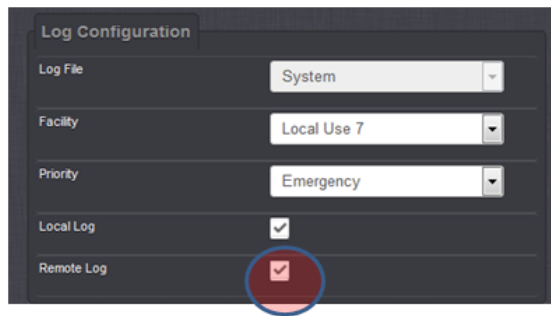
Each log of the Prisma Velasync has its own remote logging enable checkbox that also needs to be selected, if you desire for that file’s log entries to be sent to a specified syslog server.

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 Prisma Velasync/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 Prisma Velasync, 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.
- 10. Check the main default port/gateway in the configured correctly (*Management* -> *General Setup* page of the black/charcoal browser)
- 11. Perform a wireshark or tcpdump capture on the Prisma VelaSync's switch to see if syslog packets are being sent.
- 12. 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.

(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.

Issues with Syslog

1) 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)

2) 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: Internal 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.

3) 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 Jane 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."

4) 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.
13. Use tcpdump in the Prisma Velasync to verify “syslog” packets are being sent
 14. Use Wireshark to capture “syslog” packets are present.
 15. 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

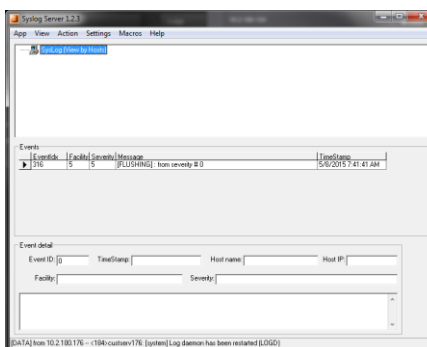
```
local7.=alert -/home/spectracom/log/events.log
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=crit -/home/spectracom/log/alarms.log
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @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\Prisma Velasync\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.

```

@packages 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
lov 5 18:37:11 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
from Time Scale: UTC to Time Scale: TAI
lov 5 18:37:31 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
from Time Scale: TAI to Time Scale: UTC
lov 5 18:37:50 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for GPS: 18
lov 5 18:37:52 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for TAI: 37
lov 5 18:38:12 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for GPS: 17
lov 5 18:38:14 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
to Time Scale Offset for TAI: 36
lov 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
lov 5 19:06:25 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
from Time Scale: UTC to Time Scale: TAI
radwin@CustService-177 /home/aspectracom/log $
```

Wireshark capture of syslog entries

Example filter can use: `ip.src==10.2.100.176` and `udp.port==514`

Example Syslog packet capture

The screenshot shows a Wireshark capture of a Syslog packet. The packet list pane displays the following entry:

No.	Time	Source	Destination	Length	Source Port	Destination Port	Protocol
1	0.000000	10.2.100.176	10.2.100.124	76	514	514	Syslog

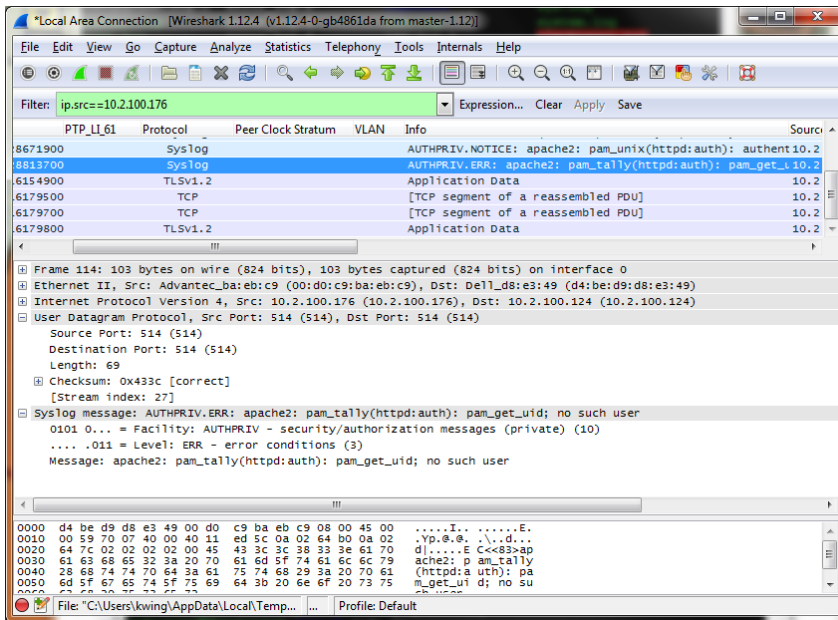
The packet details pane shows the following structure:

- Internet Protocol Version 4, Src: 10.2.100.176 (10.2.100.176), Dst: 10.2.100.124 (10.2.100.124)
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 62
- Identification: 0x3929 (13609)
- Flags: 0x00 (Don't Fragment)
- Fragment Offset: 0
- Time to Live: 64
- Protocol: UDP (17)
- Header checksum: 0x2816 (Validation disabled)
- Source: 10.2.100.176 (10.2.100.176)
- Destination: 10.2.100.124 (10.2.100.124)
- Source port: unknown
- Destination port: 514 (514)
- User Datagram Protocol, Src Port: 514 (514), Dst Port: 514 (514)
- Length: 62
- Checksum: 0x3570 (Correct)
- [Stream index: 900]
- Syslog message: LOCAL7,EMERG: Last message repeated 7 times

The packet bytes pane shows the raw data of the Syslog message:

```
0000 04 0e 09 08 03 00 00 c9 00 00 00 00 00 00 00 .....E.
0001 00 3e 35 29 40 00 00 11 28 50 00 02 64 00 00 02  :5929. (V..L.)
0002 00 61 75 02 00 00 00 18 01 70 20 13 38 14 38 00  :.....: (S...):
0003 00 61 75 74 20 00 00 72 78 41 30 00 20 72 40 70 45  :...:  :
0004 00 61 74 64 20 37 20 74 69 60 63 73 72 40 70 45  :...:  :
0005 00 61 74 64 20 37 20 74 69 60 63 73 72 40 70 45  :...:  :
0006 00 61 74 64 20 37 20 74 69 60 63 73 72 40 70 45  :...:  :
```

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.
- 16. Sys.log can only be viewed via the CLI. It's in the **home/spectracom/logs** directory
- Contains entries for syslog stopping and starting

1. Logs not present in the syslog server

17. Verify the syslog configs are correct (**Management -> Log Configuration** page of the newer browser)
18. Check main default port/gateway is correct (**Management -> General Setup** page of the newer browser)
19. Login to cli interface and try pinging out to the syslog server (could be a network issue)

B) Logs

FAQS about Prisma Velasync Logs

Q. If I delete all the log files, does the Prisma Velasync **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.**

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 7th. 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 25th, 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 7th.

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.

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.

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

- 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).

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 Prisma Velasync?

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

**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 (screenshot below from v1.0.0)

```
login as: spadmin
spadmin@10.10.224.62's password:
Linux velasync 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64
PRISMA VelaSync Version 1.0.0
Hash b8bba9817865

Last login: Fri Jun  8 17:11:40 2018 from 10.2.100.102
spadmin@velasync:~$ cd log
spadmin@velasync:~/log$ ls
alarms.log  auth.log.1  discstats  journal.log  kern.log.1  system.log  user.1
auth.log    daemon.log  events.log  kern.log     qual.log    update.log
spadmin@velasync:~/log$
```

1. 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)

B) Ability to delete the logs via the newer web browser

20. Two different locations to delete the logs:

1. 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).

2. 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).

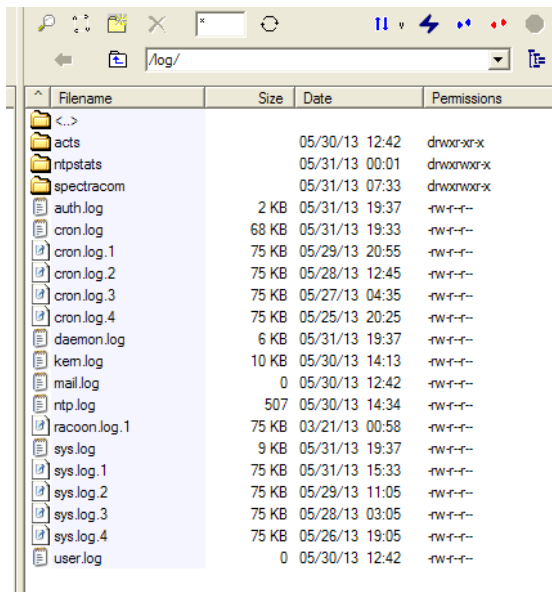
Note: The **clearlogs** command only clears the logs that are displayed in the browser (such as Qual, NTP, etc). This function does not clear the “system” logs in the background only (such as sys.log, daemon.log, kern.log, mail.log, rexd.log, cron.log, mysql_create.log and system.log)??

Log file sizes/Log rotation

- View all the logs via telnet/ssh
 1. Login 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-
racoon.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-

log 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 Prisma Velasync 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 Prisma Velasync using an FTP or SCP session.

The log bundling is controlled in the "Tools"/ "Upgrade/Backup" page of the Prisma Velasync'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 ("Prisma Velasync.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):



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) web browser

Management -> Log Configuration page, Center "Gear" ICON for each log type.

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

1. Using new (black/charcoal) browser (versions 5.1.2 and above)

All of the Prisma Velasync'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 Prisma Velasync 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 Prisma Velasync'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 "Prisma Velasync.log".

B) Save logs via CLI interface only (not using the web browser)

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 Prisma Velasync 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 $ █
```

3. 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 $ █
```

4. Use an FTP program (such as CoreFTP lite freeware) or SCP out the files.

Important Note: Transfer out this file using **Binary** mode

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 Prisma Velasync'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 Prisma Velasync 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 Prisma Velasync'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 ("Prisma Velasync.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

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 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)

- clearlogs CLI command

C) 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 Versa sent the raw log entries to the Syslog server

- Each log entries contain the DNS Hostname of the Versa.

Available Log files in 1232 VelaSync

- At least the initial VelaSync release (Version 1.0.0/1.1.0) has limited log files/log entries (as compared to SecureSyncs)
 - Not all Log files are available.
 - Some Log files (such as “NTP” for instance) are present, but remain empty (contain no entries)

1. alarms.log (Alarms log)

2. events.log (Events log)

- This log file is always empty in at least versions 1.0.0/1.1.0 ??

3. qual.log (Qual log/Qualification log)

(27 Feb 2019) Observed software issue in at least v1.1.0 of Velasyncs (“Q=” value not always “Q=3600” for an entirely qualified hour) though no reboots occurred Refer to Salesforce Case 186801 for examples.

Example entry: Feb 24 12:00:02 [711]: GPS 0: 13 = 124 14 = 1049 15 = 1865 16 = 561 Q = 3599

Email report from Keith to Denis/Dave S (26 Feb) Just to add to Morgan's request for 1232 VelaSync log review from this afternoon (reported Timing System Hardware error on Case 186801 for DV Trading) note this appears to be legacy 1225 VelaSync which has been retrofitted to become a 1232 Velasync (its Serial Number is 631R).

4. journal.log (Journal log)

5. kern.log (kernel log)

6. ntp.log (NTP log)

7. osc.log (Osc log/Oscillator log)

- This log file is always empty in at least VelaSync versions 1.0.0/1.1.0
- Refer to the [discstats](#) files as an alternative source of info

8. system.log (System log)

9. timing.log (Timing log)

21. refer to ublox receiver section info in: [..\CustomerServiceAssistance.pdf](#)

System messages

1. constant messages (every 3-10 seconds) “Using degraded feature set (UDP) for DNS server 8.8.8.8”.

2020-03-02T11:50:50+00:00 fts-01 systemd-resolved[756]: Using degraded feature set (UDP) for DNS server 8.8.8.8.
2020-03-02T11:50:54+00:00 fts-01 systemd-resolved[756]: Using degraded feature set (TCP) for DNS server 8.8.4.

- Refer to Salesforce case 225962 (March 2020)
- Observed with version 1.3.1C installed
- Fixed by setting the gateway address to 0.0.0.0 (see emails below)
- Suspect this will be fixed in either the version 1.4.1 or 1.4.2 update.

(email Keith sent to them for a different reason Quick question for you: Is the physical switch configured as the gateway address “x.x.x.1” currently reachable by the VersaSync, over the network?)

Note that with the current version of software, the VersaSync needs to be able to actively reach the configured default gateway address, to allow communications with other devices that are even on its same subnet (not just devices on the other side of the gateway),,

For a direct connection to the VersaSync (where the configured gateway address isn't reachable via the network connection) the gateway address in the VersaSync currently needs to be configured as 0.0.0.0. .

The pending software update for the VersaSync is removing the need for the gateway to be reachable, in order to communicate with other devices on its same subnet.

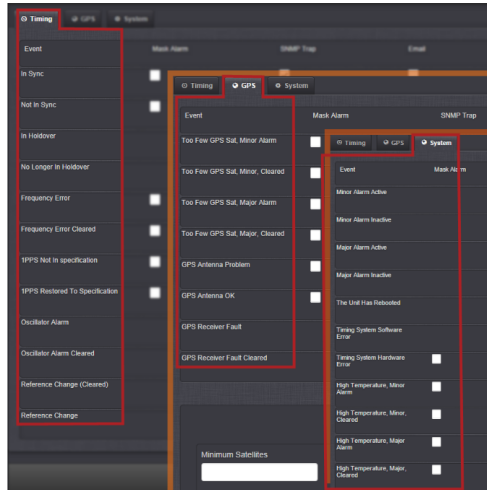
A (reply from customer) That did it!!!! I set the default gateway for eth0 & eth1 to 0.0.0.0 and all of the “Using degraded feature” messages have disappeared!

Notifications / Email alerts /SNMP

NOTE (13 Apr 2021): this entire section primarily copy/pasted from 1200 SecureSync Assist doc Needs editing!!

- Refer to the online VersaSync user guide at:
http://manuals.spectracom.com/VSS/Content/NC_and_SS/Com/Topics/SETUP/SNMP_Intro.htm?

*Notifications (SNMP traps and email alerts)/Alarms



Configuration for Notifications (SNMP Traps and/or Emails) to be sent

- Refer to the online SecureSync user http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/Notifications.htm

Web browser

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)

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

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):

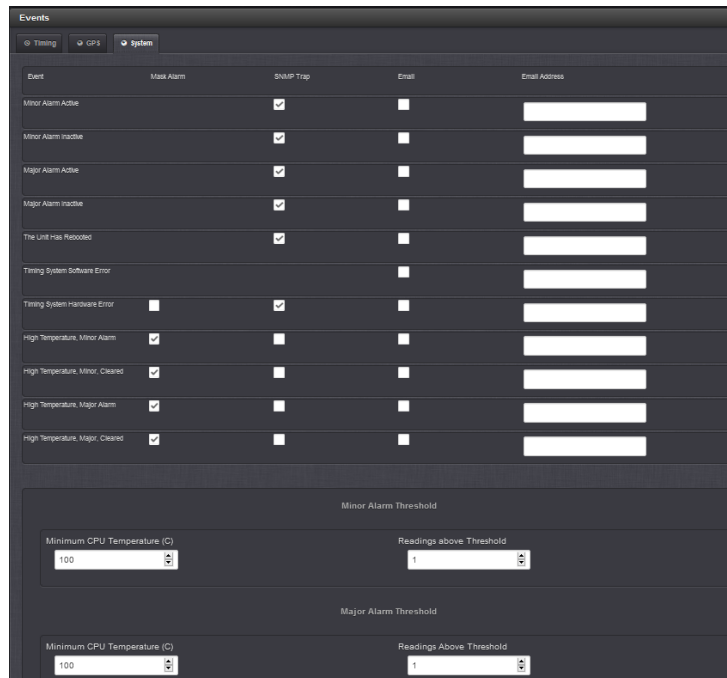
Opt-IDM: available Broadshield notifications (v5.7.1 and above only, and only with Opt-IDM enabled)

- 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



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
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

```

System log entries associated with Management -> Notifications page configuration

- **In at least version 5.4.1, submitting any changes in the Management -> Notifications page will result in the following group of log entries being asserted in the system.log file.**

```
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)
```

****Nullmailer/Email Alerts**

B) Nullmailer:

From 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
- 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.

A) 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 for SecureSyncs):

22. At: [\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP](#)

23. 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.

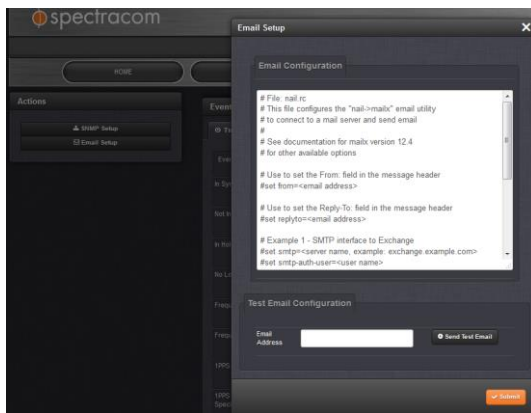
Set autocc=<email address 1>,<email address2>,...

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.

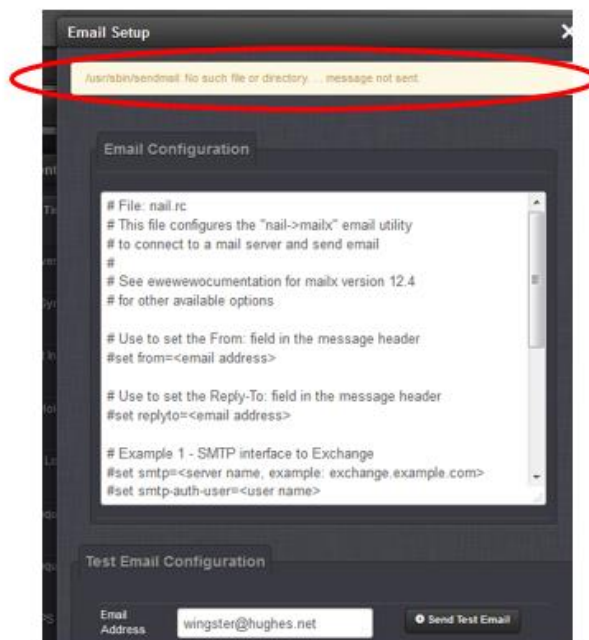
B) web browser

Management -> **Notifications** page of browser

A) 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.

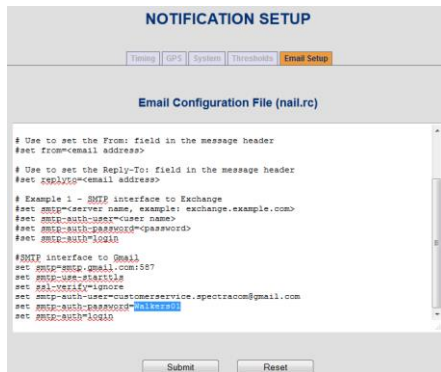
1. Example smtp setup for Outlook 365 SMTP from a workstation that worked for Keith

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 or 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
```

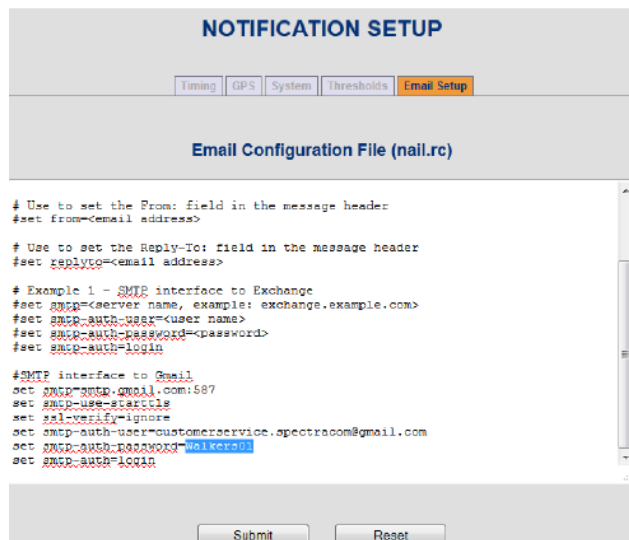
Testing testing testing

<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 in a SecureSync (performed by Sam Otto)



"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

- Like 1200/2400 SecureSyncsVersaSyncs also use 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 in VersaSync (ascending order) ??

Versa System Version	Corresponding Net-SNMP Version	Notes
		None that I am aware of, as of at least 1.4.2/1.3.0 (for IRIG AM)

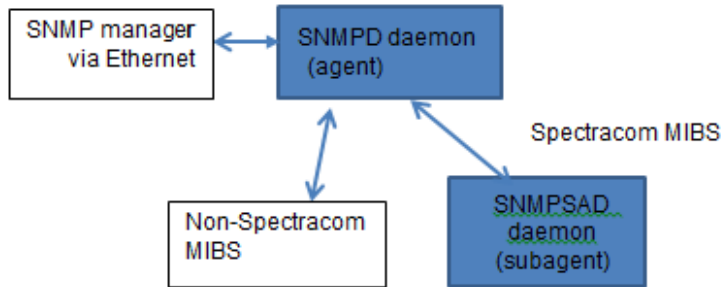
SNMP MIB files/Object IDs

- **Path to the MIB files stored in the Model 9400 series:** Home/Spectracom/mibs
- A)** The SNMP object numbers of ".1.3.6.1.4.1.18837." are for the Spectracom-specific objects.
- B)** The SNMP object numbers of ".1.3.6.1.4.1.8072." are objects associated with Net-SNMP.
- C)** 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:
 - A) SNMPD:** the agent running in the Linux OS
 - B) SNMPSAD:** the subagent running in Spectracom application
 - C) 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>

D) Newer web browser: *Management* -> *SNMP Setup* page

E) 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

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

- A) be **8 to 32** characters (earlier rev SecureSync Manual incorrectly stated “between 4 and 32 characters in length.”)

2. SNMPv3 user configuration

Newer web browser

SNMPv3 Settings

User Name: rererere

Auth Type: MD5

Auth Passphrase:

Priv Type: DES

Priv Passphrase:

Permissions: Read/Write

Delete Submit

SNMPv3 User name (username) field

Enter the **8 to 32-character** user (principal) on whose behalf the message is being exchanged
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 (in SecureSyncs)

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 web browser requirement)

- **Per:** <http://net-snmp.sourceforge.net/docs/README.snmpv3.html>

WARNING: SNMPv3 pass phrases must be at least 8 characters long!

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
- Refer to the SecureSync SNMP Tech Note: [I:\Customer_Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP](I:\Customer_Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\SNMP-Notifications-email_alerts\SNMP)

A) SNMPV3 traps (note the Versa 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

SecureSync 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

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**”)
 - A) 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
 - B) 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 manger.

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 verisons 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 convieniece 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
- 3) Type the following command **15.108.10**
- 4) <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 snmpptest 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 ~ $
```

- 5) 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"

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 shows an SNMP Manager interface with a tree view on the left and a configuration panel on the right. The tree view shows the hierarchy: snmpFrameworkMIBObjects > snmpEngine > snmpEngineID. The configuration panel shows the following details for snmpEngineID:

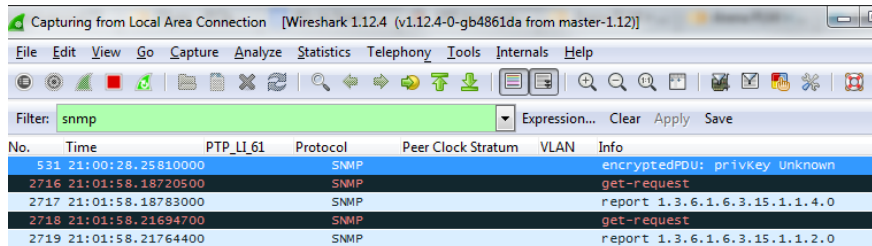
Object ID	Description
.1.3.6.1.6.3.10.2.1.1	"An SNMP engine's administratively-unique identifier. This information SHOULD be stored in non-volatile storage so that...

The configuration panel also shows a list of other SNMP objects and their values, such as #OutNUcastPkts.6 through #OutNUcastPkts.8, #OutDiscards.1 through #OutDiscards.8, #OutErrors.1 through #OutErrors.8, #OutQL.en.1 through #OutQL.en.8, and #Specific.1 through #Specific.8. The status of snmpEngineID is 'current' and its access is 'read-only'.

- 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_LL61	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)

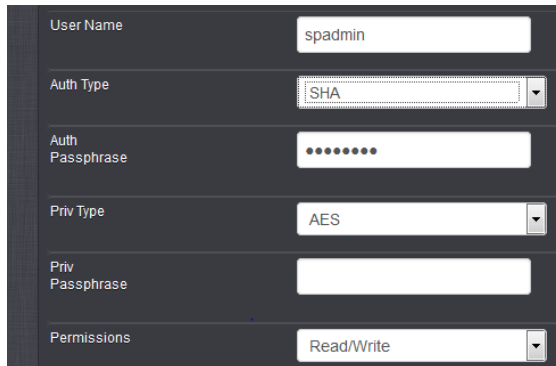
- update version 5.8.5 update now retains engine ID on each startup

C) **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).

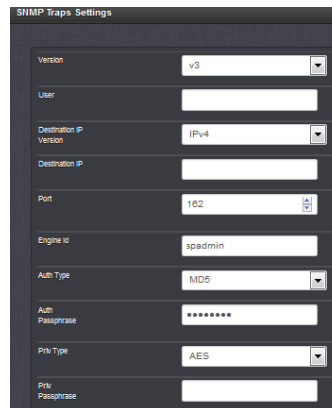
A **Keith's response:** Correct. SecureSync is authpriv only. You can set Permissions in the snmpV3 section of the Management -> **SNMP Setup** page of the browser, to read or read/write (as shown in the screenshot below). If the user wants to setup the 'Trap only' user, it does not have to be reflected 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



User Name	spadmin
Auth Type	SHA
Auth Passphrase	••••••
Priv Type	AES
Priv Passphrase	••••••
Permissions	Read/Write

Users for Traps



Version	v3
User	
Destination IP Version	IPv4
Destination IP	
Port	162
Engine id	spadmin
Auth Type	MD5
Auth Passphrase	••••••
Priv Type	AES
Priv Passphrase	••••••

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).

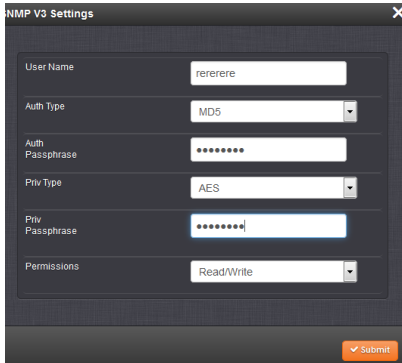
“User name” field

A) **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.

B) **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”)

Setting up ManageEngine SNMP Manager to work with SNMPv3 traps from SecureSync

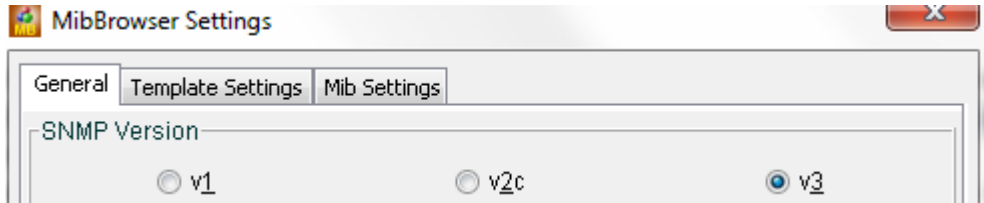
1. In the **Management -> SNMP** page of the SecureSync, Add/Configure a new V3 user (note this is not required to send a v3 trap that wireshark can see, but is required for the SNMP manager to be able to authenticate/see the trap). Use the same user name that is used for the V3 user name (example below uses “**rererere**”)



The image shows the 'SNMP V3 Settings' dialog box. It contains the following fields and options:

- User Name:
- Auth Type:
- Auth Passphrase:
- Priv Type:
- Priv Passphrase:
- Permissions:
- Buttons:

2. Select “**V3**” at the top of the top of the “General tab” of the ManageEngine GUI

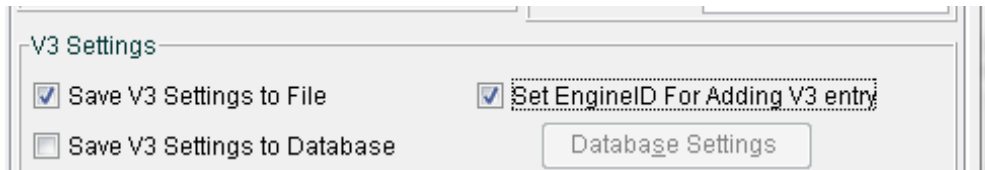


The image shows the 'MibBrowser Settings' dialog box, specifically the 'General' tab. Under the 'SNMP Version' section, the 'v3' radio button is selected.

SNMP Version

v1 v2c v3

3. Select the checkboxes for both “**Save V3 Settings to file**” and “**Set EngineID for adding V3 entry**”

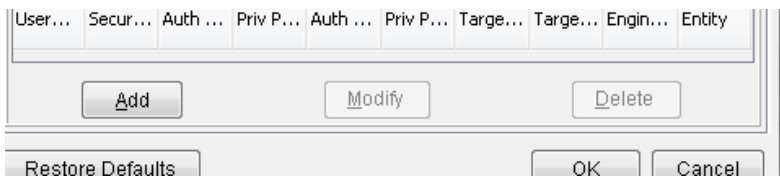


The image shows the 'V3 Settings' dialog box. The following checkboxes are checked:

- Save V3 Settings to File
- Set EngineID For Adding V3 entry
- Save V3 Settings to Database

Buttons:

4. Press the “**Add**” button in the bottom left corner to add a “v3 user”

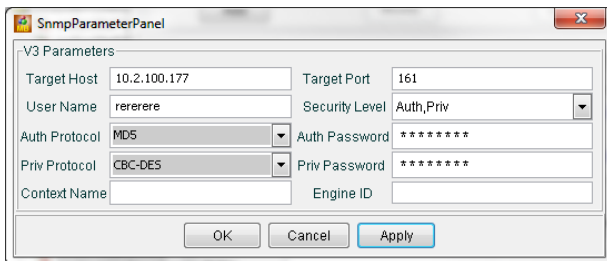


The image shows the 'SNMP User Management' dialog box. The 'Add' button is highlighted in the bottom left corner.

Buttons:

Buttons:

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).



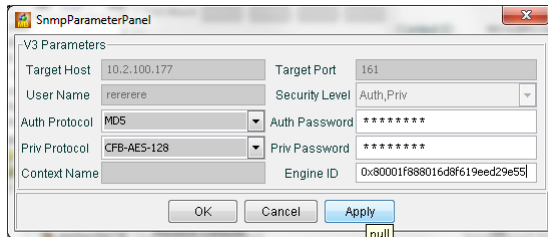
The image shows the 'SnmpParameterPanel' dialog box. The following fields are filled:

- Target Host:
- Target Port:
- User Name:
- Security Level:
- Auth Protocol:
- Auth Password:
- Priv Protocol:
- Priv Password:
- Context Name:
- Engine ID:
- Buttons:

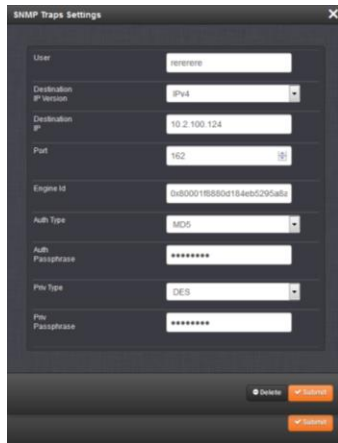
- With Auth and Priv protocols and passwords matching the SecureSync's SNMPv3 user section, the context ID field in the main page (General tab) of the manageengine gui will be generated.



- 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.



E) 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:

C) [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 advise 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.

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 /etc
spectracom@Spectracom111 ~$ cd config
spectracom@Spectracom111 ~$ cd /etc/snmp
spectracom@Spectracom111 ~$ cat snmpd.conf
#-----
#com2sec sec.name source community
#-----
com2sec comuser_3 default snmpstatAlpha
com2sec comuser_4 default snmpstat
#-----
#group groupname sec.model sec.name
#-----
group rwnoauthgroup v2c comuser_3
group rwnoauthgroup v2c comuser_4
group rwprivgroup v1 snmpv3test
group rwprivgroup v1 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 rwauthgroup "" 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 1234567843434334 AES 1234567843434334
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

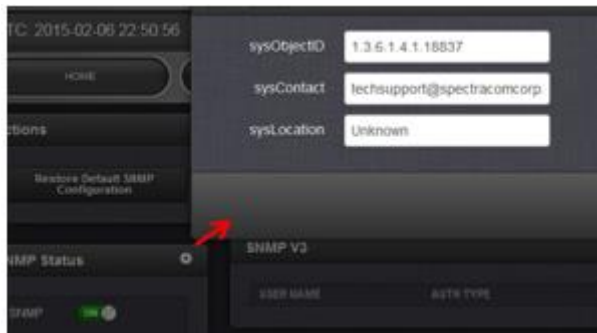
- **SysObjectID:** The three values can be changed from the default values if desired.

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)
 - D)** 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.
 - E)** 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:

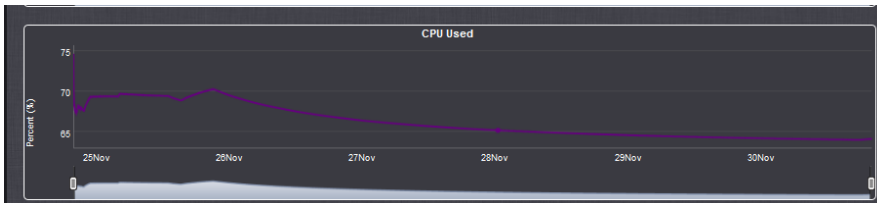


CPU usage (CPU used) / Processor usage/CPU usage 100%

- Refer to Mantis case 3029.
 - CPU usage is a comparison of processor “use time” versus “rest time”.
- A) 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.
 - B) 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.
 - C) 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)

- A) CPU usage graph was added in **version 5.3.1**
- B) Located at the bottom of the **Tools ->System Monitor** page of the newer browser (not available in classic interface).
- C) 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.



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)).**
- D) Data for this graph is located (can be viewed) in the “**log_sys_mons**” table, “**cpu_used**” column
 - E) 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 snmp-test 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

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)
 - F) Associated segfaults were asserted in keern.log
 - G) 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	snmpget	IPv4	default

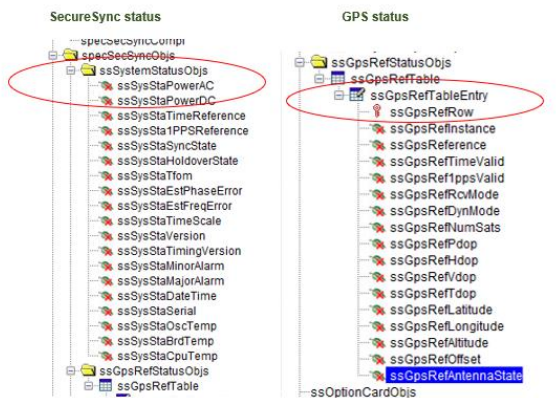
- Refer to: <http://en.wikipedia.org/wiki/Net-SNMP>

https://docs.oracle.com/cd/E19201-01/820-6413-13/SNMP_commands_reference_appendix.html#50446362_54136

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 1.3.6.1.4.1.18837.3.2.2.1.1.17.0 <enter>** (where **XXXXXXX** is the v2c community name, and where **Y.Y.Y.Y** is the SecureSync's IP address).

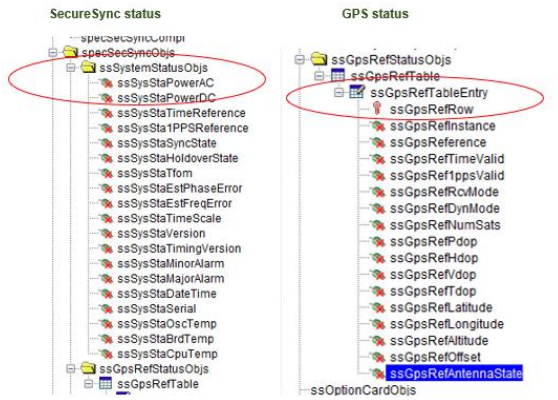
Below is an example command, and the expected response: (Note the first word is **snmpwalk**, instead of the usual word **snmpget**)

`snmpwalk -v 2c -c snmpptest 10.15.108.12 .1.3.6.1.4.1.18837.3.2.2.2.1.1.17`

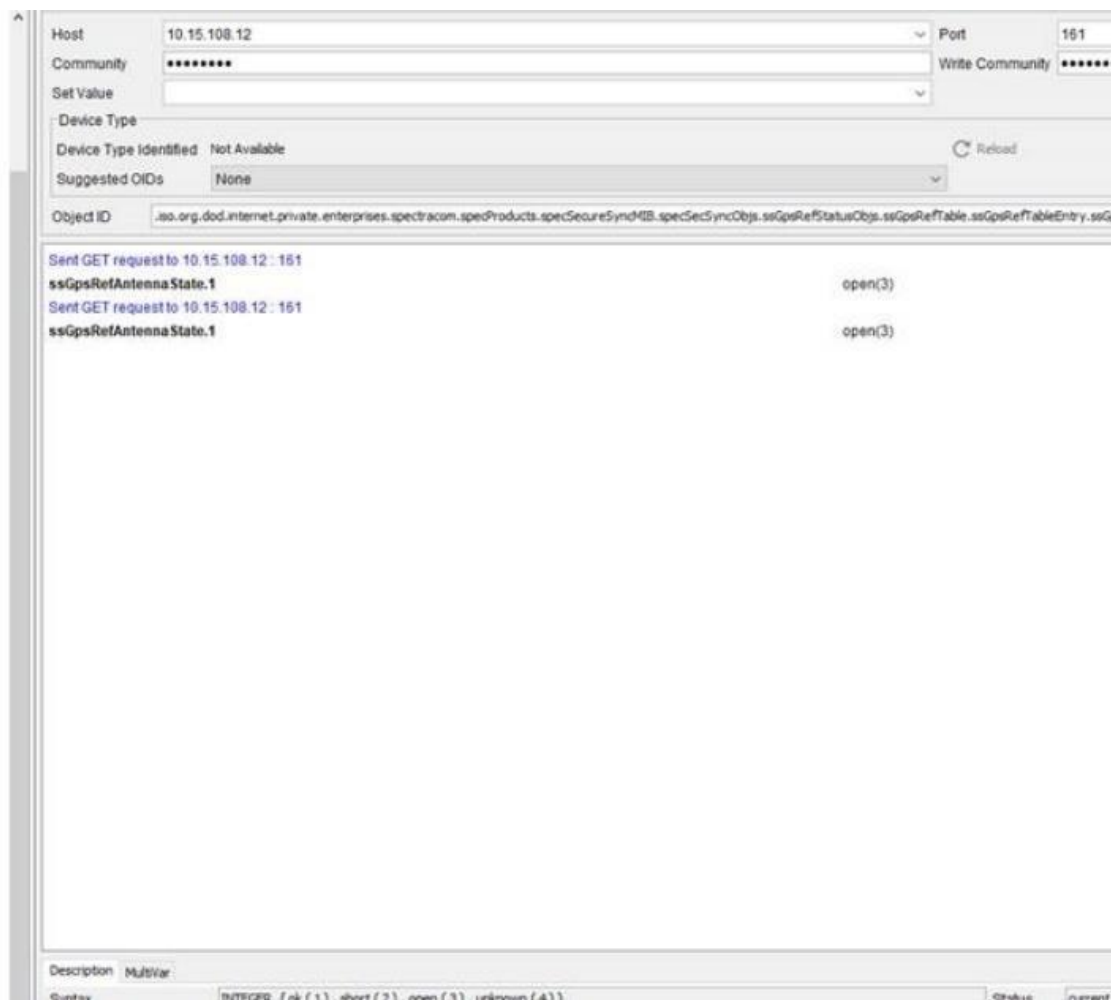
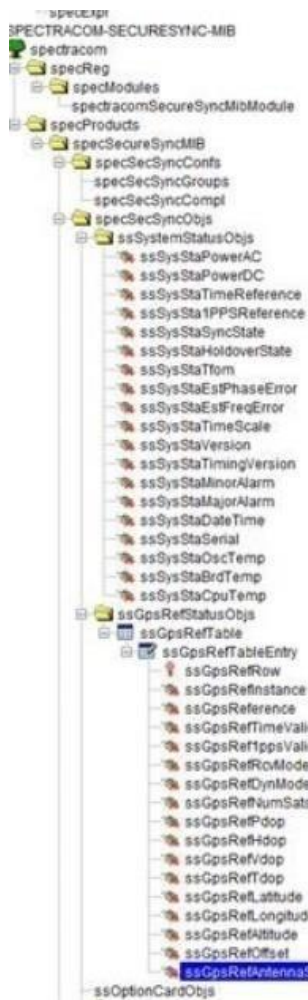


Here is the explanation why the command needs to be `snmpwalk`, instead of `snmpget` (based on my testing)

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 snmptest 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:

```
spadmin@Spectracom ~ $ snmpwalk -v 2c -c snmptest 10.15.108.12 .1.3.6.1.4.1.18837.3.2.2.2.1.1.17
SNMPv2-SMI::enterprises.18837.3.2.2.2.1.1.17.1 = INTEGER: 3
spadmin@Spectracom ~ $
```

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
RFC1213-MIB::ifIndex.3 = INTEGER: Serial0/0
RFC1213-MIB::ifIndex.4 = INTEGER: Serial0/0
RFC1213-MIB::ifIndex.5 = INTEGER: Serial0/0
RFC1213-MIB::ifIndex.6 = INTEGER: Serial0/0
RFC1213-MIB::ifIndex.7 = INTEGER: Serial0/0
RFC1213-MIB::ifIndex.8 = INTEGER: Serial0/0
RFC1213-MIB::ifIndex.9 = INTEGER: Serial0/0
RFC1213-MIB::ifIndex.10 = 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 snmptest 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

F) 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 snmptest 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

G) 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**

H) 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)

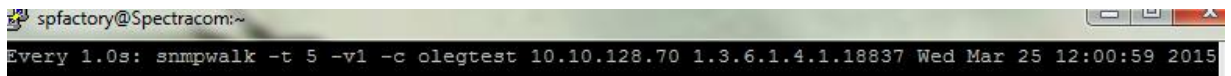
I) Just once

(Type): **snmpwalk -t5 -v2c -c snmpctest 10.2.192.226 1.3.6.1.4.1.18837**

J) Example to repeatedly walk the entire MIB, once per second:

(Type): **watch -n1 snmpwalk -t5 -v2c -c snmpctest 10.2.192.226 1.3.6.1.4.1.18837**

Note: the time at the top will increment each second



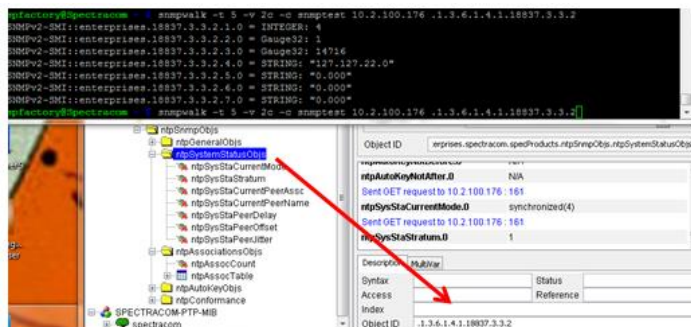
```
spfactory@Spectracom:~  
Every 1.0s: snmpwalk -t 5 -v1 -c olegtest 10.10.128.70 1.3.6.1.4.1.18837 Wed Mar 25 12:00:59 2015
```

K) Walk just one MIB such as NTPSystemStatysObjsMIB (with a 5 second timeout)

(Type) **snmpwalk -t 5 -v 2c -c snmpctest 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)



L) 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**

M) 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

N) Get the system uptime

(Type the following): **snmpget -v 2c -c snmpptest 10.15.108.11 SNMPv2-MIB::sysUpTime.0**

```
pfactory@Spectracom ~ $ snmpget -v 2c -c snmpptest 10.2.100.176 SNMPv2-MIB::sysUpTime.0
ISMN-EVENT-MIB::sysUpTimeInstance = Timeticks: (526358) 1:27:43.58
```

O) 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.

A) 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

GPS status



- 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")	.1.3.6.1.4.1.18837.3.2.2.2.1.1.17	spe
# Satellites being tracked ("ssGpsRefNumSats")	.1.3.6.1.4.1.18837.3.2.2.2.1.1.8	spe
GPS Time validity ("ssGpsRefTimeValid")	.1.3.6.1.4.1.18837.3.2.2.2.1.1.4	spe
GPS 1PPS validity ("ssGpsRef1ppsValid")	.1.3.6.1.4.1.18837.3.2.2.2.1.1.5	spe
GPS latitude ("GpsRefLatitude")	.1.3.6.1.4.1.18837.3.2.2.2.1.1.13	spe
GPS longitude ("ssGpsRefLongitude")	.1.3.6.1.4.1.18837.3.2.2.2.1.1.14	spe
GPS Altitude ("ssGpsRefAltitude")	.1.3.6.1.4.1.18837.3.2.2.2.1.1.15	spe

```
spadmin@Spectracom ~$ snmpgetnext -v 2c -c snmpptest 10.15.108.12 .1.3.6.1.4.1.1.18837.3.2.2.2.1.1.17
SNMPv2-SMI::enterprises.18837.3.2.2.2.1.1.17.1 = INTEGER: 3
spadmin@Spectracom ~$
```

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

H) 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

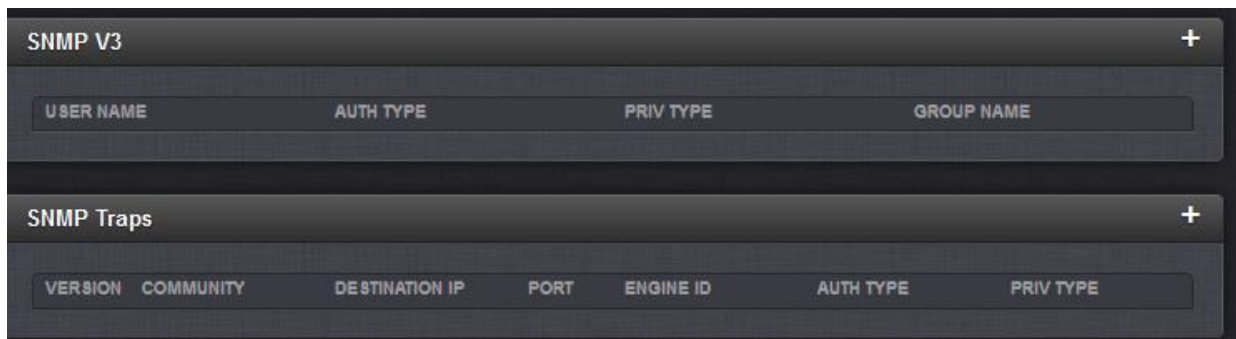
- engineID now retained when restoring SNMP (v5.8.5 and above, July 2019)

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

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

P) “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.

I) “noAuthnoPriv”: Messages can be sent unauthenticated and unencrypted (this mode is unsecure/not supported in SecureSync)

J) “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)

Q) Authentication (“Auth Type” field)

- **Auth Type:** supports MD5 or SHA (no selection available for ‘none’)

B) 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)

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 (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/mailling.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 "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

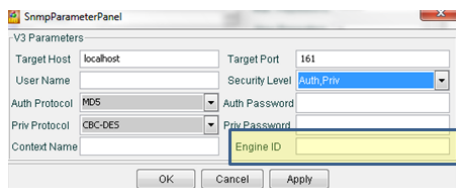
- Refer to Salesforce Cases such as **188893**
- Refer to JIRA ticket **SSS-258**
- Expected to be addressed in update v5.8.5

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)

- K) Versions 4.8.9 and above:** 50 characters
- L) 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)

- A) **Model info:** Not available in versions 5.2.1 and below. Refer to Mantis case 1855.
- B) **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.
- C) **Installed software version** (ssSysStaVersion):
- D) **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)
- E) **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:

F) SecureSyncs: Version 5.2.0 software now correctly responds with the installed version number.

G) 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.

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.

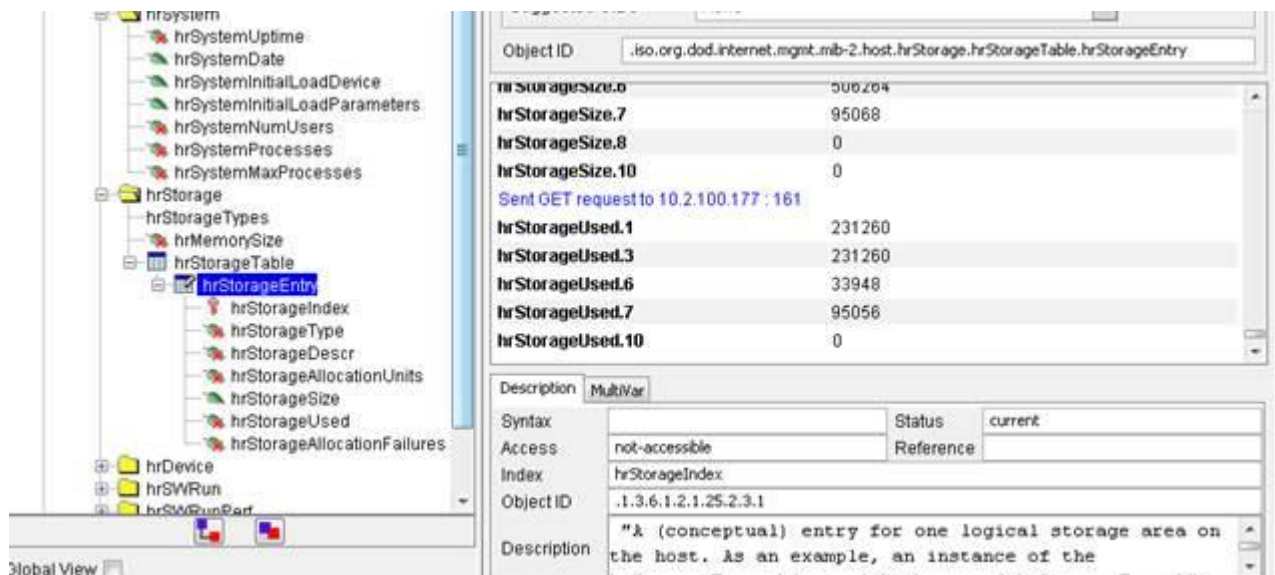
Set

	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

Note: testevent commands do work with snmpv3, as observed during 1.5.0 Beta update testing,

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):

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 \(wireshark for Linux\)](#)

A) Some examples below:

Note **VersaSync software versions of at least 1.4.2 (and Beta v1.5.0)** require the word **sudo** be added before each tcpdump command (as found by Keith during beta v1.5.0 testing)

To capture data on specific Ethernet interfaces

- A) To capture traffic on **eth1** instead of default port of eth0: **sudo tcpdump -i eth1**
- B) To capture traffic on more than one interface (such as **eth0** and **eth1**): **sudo tcpdump -i eth0 -i eth1**
- C) 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

- A) NTP on eth0: **sudo tcpdump port 123** (no need to define interface as eth0 is default)
- B) Radius on eth0: **sudo tcpdump port 1812 and 1813** (no need to define interface as eth0 is default)
- C) LDAP on eth0: **sudo tcpdump port 389 and 636** (no need to define interface as eth0 is default)
- D) Syslog on eth0: **sudo tcpdump port 514** (no need to define interface as eth0 is default)
- E) PTP on eth0: **sudo tcpdump ports 319 and 320** (no need to define interface as eth0 is default)
- F) 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.oroia.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.oroia.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

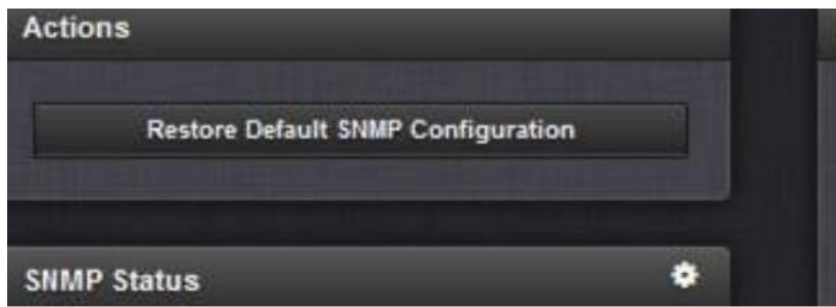
A) General SNMP troubleshooting

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 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

A) New Web browser: **Management** -> **SNMP Setup** page

B) 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: 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 snmpptest 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”

Note: rc-status command apparently not valid on Versas (as shown below, on beta v1.5.0)

```
spadmin@versasync-0c028e:~$ rc-status
-bash: rc-status: command not found
spadmin@versasync-0c028e:~$
```

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
```

- A) 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.
- B) 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

- Refer to the tcpdump section of this doc for more info

SNMP Traps sent to any Ethernet interface:

- (at least Versions 1.4.2 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" [Iscoped PDU]c5_
ec_a0_af_3d_f3_ec_4e_0e_87_3f_03_e5_a9_fb_01_95_53_c9_32_aa_c1_05_03_2e_0b_69_3a_73_3e_29_da_14_ac
43_d8_7d_72_c3_36_70_97_37_b2_90_a5_aa_8e_76_47_1a_9f_45_5b_1c_83_05_f2_1b_31_4c_25_cf_10_b4_fc_4
7_12_f8_59_a2_ee_5d_1e_91_35_91_1e_77_12_47_eb_2d_4c_54_53_f6_a3_8c_f7_00_47_42_f7_b3_a9_70_07_3f_
92_e7_5d_a7
15:21:47.189748 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [Iscoped PDU]f1_
ae_cd_4c_c3_19_9a_8d_68_e8_f8_50_8a_83_6b_f0_29_65_c3_6e_4d_4e_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_99_2f_be_02_04_cb_24_12_29_02_b9_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
15:21:47.325695 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [Iscoped PDU]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_6d_10_4c_64_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_fa_29_a1_ca_16_c8_ad_
7c_01_b3_a4_ee_8e_8e_c9_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 (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 it’s 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
15:21:09.459717 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [Iscoped PDU]c5_
ec_a0_af_3d_f3_ec_4e_0e_87_3f_03_e5_a9_fb_01_95_53_c9_32_aa_c1_05_03_2e_0b_69_3a_73_3e_29_da_14_ac
43_d8_7d_72_c3_36_70_97_37_b2_90_a5_aa_8e_76_47_1a_9f_45_5b_1c_83_05_f2_1b_31_4c_25_cf_10_b4_fc_4
7_12_f8_59_a2_ee_5d_1e_91_35_91_1e_77_12_47_eb_2d_4c_54_53_f6_a3_8c_f7_00_47_42_f7_b3_a9_70_07_3f_
92_e7_5d_a7
15:21:47.189748 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [Iscoped PDU]f1_
ae_cd_4c_c3_19_9a_8d_68_e8_f8_50_8a_83_6b_f0_29_65_c3_6e_4d_4e_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_99_2f_be_02_04_cb_24_12_29_02_b9_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
15:21:47.325695 IP 10.15.108.10.55761 > 192.168.1.79.snmptrap: Fmap U="snmptrap" [Iscoped PDU]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_6d_10_4c_64_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_fa_29_a1_ca_16_c8_ad_
7c_01_b3_a4_ee_8e_8e_c9_35_5b_5d_10_c6_3d_0c_f5_40_86_65_72_b9_bc_b8_a1_4c_db_6e_6e_47_5d_fe_68
```

- 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)

1) 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.
-

2) (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.

3) 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!!!

4) 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.
-

5) 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.

6) 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.

7) 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
```

8) 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.

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(1),
                          noholdover(2) }
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION     "Status of the unit's holdover with its time/lpps
references."
 ::= { ssSystemStatusObjs 6 }

```



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!!

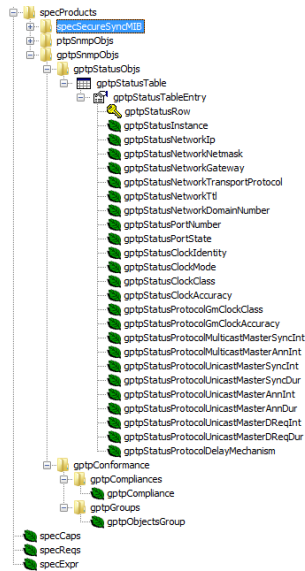
If you have the earlier iteration of the MIB file, there are two ways to obtain it. The attached document discusses how to FTP/SCP transfer it out of the SecureSync. Or for your convenience, I have attached it for you. Uninstall the earlier from the Manager and install the latest,. Recompile the MIBs and I highly BELIEVE you will finally be all set.

Examples of available SNMP Gets/Sets

PTP mib file (for 1204-12 10/100 card) and GB PTP mib file (for 1204-32 card)

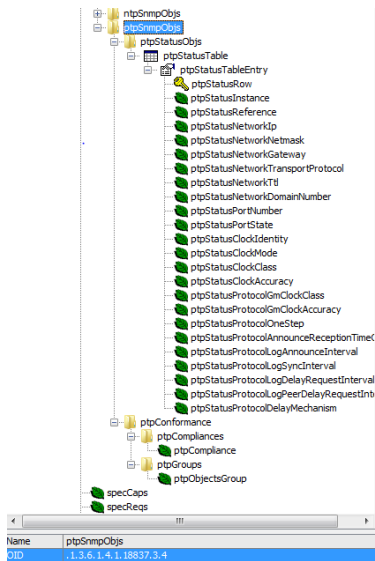
C) “SPECTRACOM-GPTP.mib” file/objects (starts with .1.3.6.1.4.1.18837.3.5)

- 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)



D) 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)



E) 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	(SnmP 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):

- C) The ifDescr object lists all of the available interfaces in the time server and reports the “assigned name” for each one.

ifOperStatus	ifDescr	ifOperStatus.1	up(1)
ifAdminChange	ifDescr.2	ifOperStatus.2	down(2)
ifOutQueue	ifDescr.3	ifOperStatus.3	down(2)
ifInQueue	ifDescr.4	ifOperStatus.4	down(2)
ifInCastPkts	ifDescr.5	ifOperStatus.5	up(1)
ifOutCastPkts	ifDescr.6	ifOperStatus.6	up(1)
ifInErrors	ifDescr.7	ifOperStatus.7	down(2)
ifOutErrors	ifDescr.8	ifOperStatus.8	down(2)
ifDiscards			
ifUnknownProtos			
ifMulticastPkts			
ifBroadcastPkts			
ifDiscards			
ifOutErrors			
ifInErrors			
ifOutQueue			
ifSpecific			

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 ☺!)

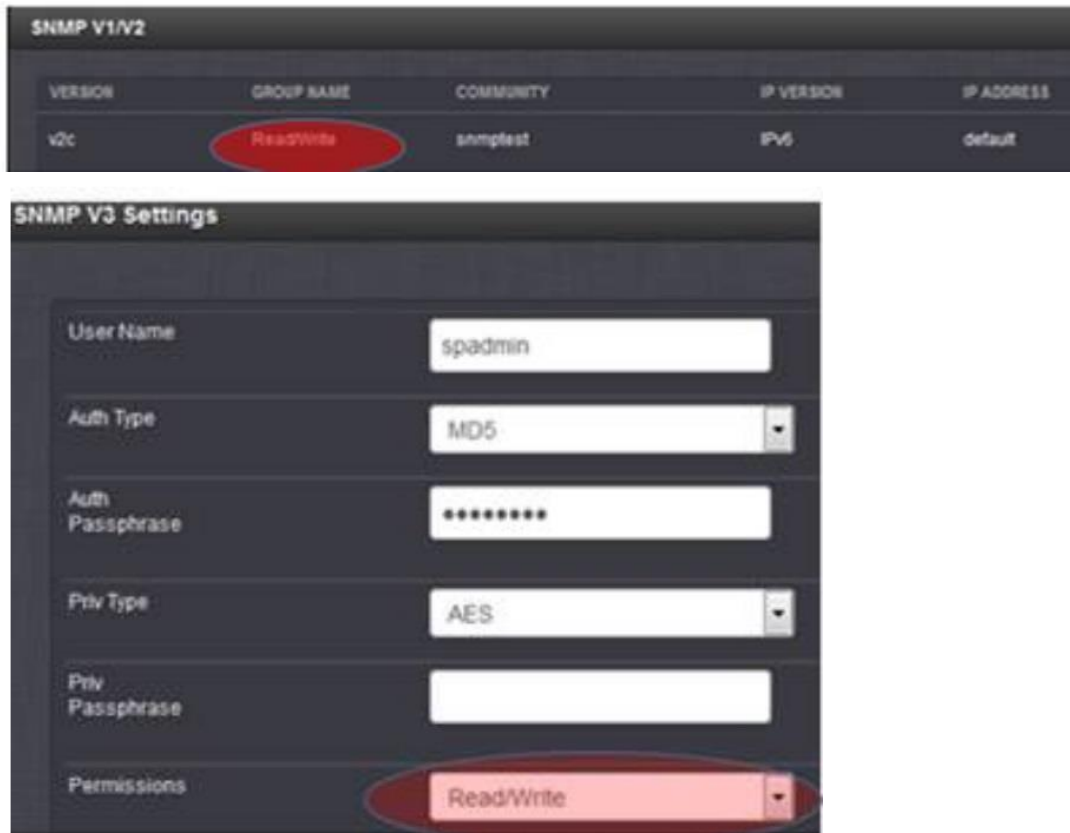
The “Enable/Disable” and “Priority” fields of the “Reference Priority Setup” can be configured via the SecureSync’s web browser or with SNMP “Sets”. The “SPECTRACOM-SECURE-SYNC-MIB.mib” file contains the applicable values for configuring this table via SNMP. Refer to “**ssReferenceMgmtObjs Objects [enterprises.18837.3.2.2.4.x]**” 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.

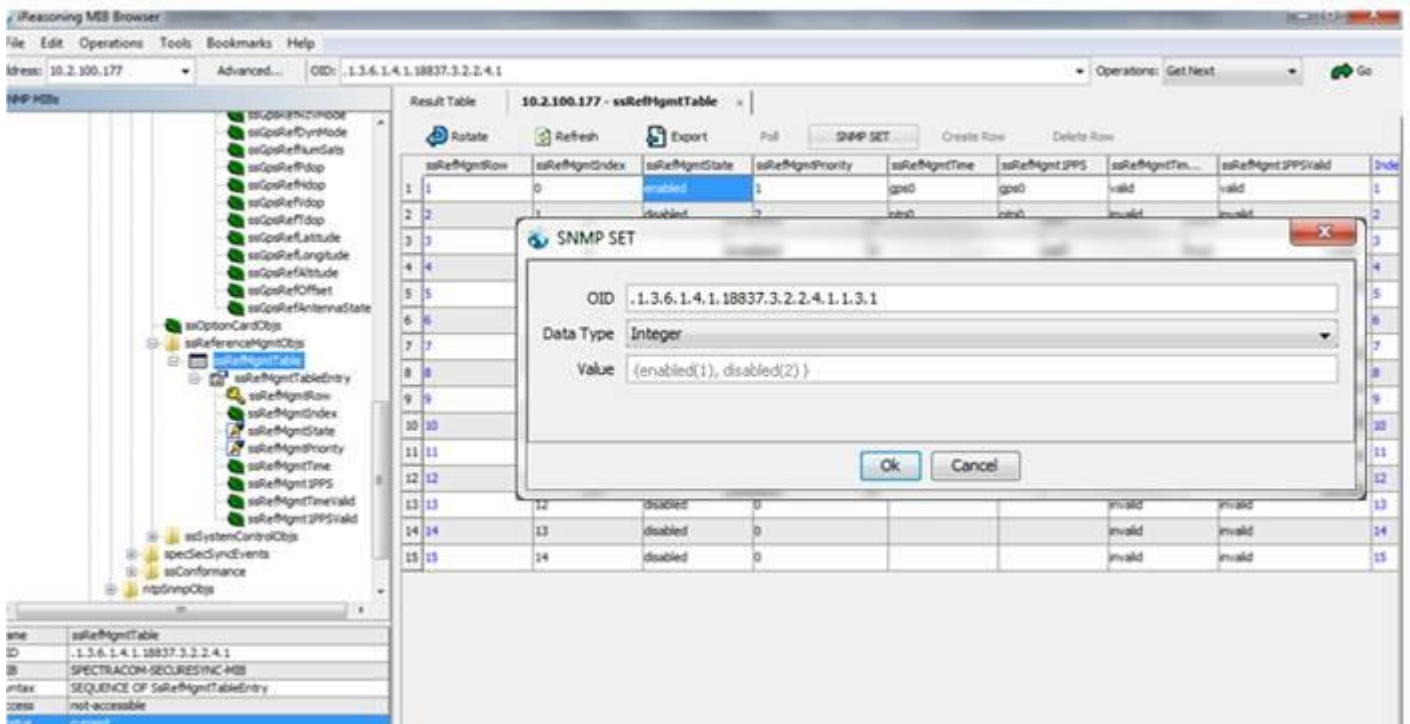
Per the “Note” above, the SecureSync’s input reference priority table should initially be pre-configured (using the **Management -> Reference Priority** page of the web browser) with a “list” of all input references that the SecureSync could potentially be synced with. Thereafter, SNMP can then be used 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



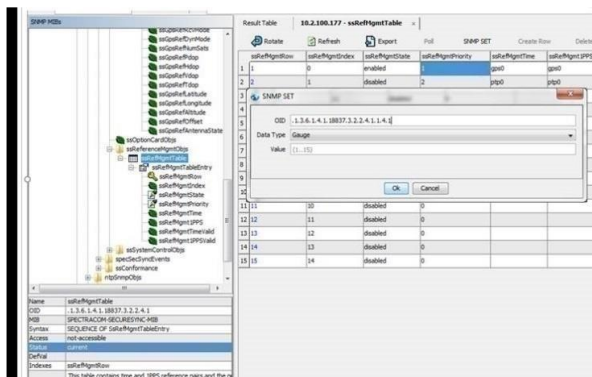
Below are the specific OIDs to enable/disable each reference.

Index (row of table)

- A) .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.1
- B) .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.2
- C) .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.3
- D) .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.4
- E) .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.5
- F) .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.6
- G) 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)

- H)** .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.1
- I)** .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.2
- J)** .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.3
- K)** .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.4
- L)** .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.5
- M)** .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.6
- N)** 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

A) 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

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)
- B) Note:** NOT in Arena, as it’s an FOUO document: [\rocuso.uso.oroiausa.com/us-only/Documentation/Released/Manuals/1200-xxxx-xxxx](http://rocuso.uso.oroiausa.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](#)